ON THE EXISTENCE OF A PRIMITIVE (PROPERLY OR IMPROPERLY) TERNARY QUADRATIC FORM ASSOCIATED WITH A GIVEN DETERMINANT

By

SYED ASADULLA

A DISSERTATION PRESENTED TO THE GRADUATE COUNCIL OF
THE UNIVERSITY OF FLORIDA
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE
DEGREE OF DOCTOR OF PHILOSOPHY

UNIVERSITY OF FLORIDA
August, 1966

Dedicated to my mother and to my wife

ACKNOWLEDGMENTS

The author wishes to express his sincere appreciation to Dr. E.H. Hadlock, chairman of his supervisory committee, for his genuine interest, encouragement and continued assistance in the preparation of this dissertation. He wishes to thank Dr. J.E. Maxfield, chairman of the Department of Mathematics and a member of his committee, for his guidance and assistance throughout the author's stay at the University of Florida. He also wishes to thank the other members of his committee, Dr. T.O. Moore, Dr. W.R. Hutcherson and Dr. W.O. Ash for their help and encouragement.

TABLE OF CONTENTS

PAGE

ACKNOWLEDGMENTS iii

Chapter

I. INTRODUCTION 1

II. FORMULAS FOR s_i, r_j AND c_1 AND VERIFICATION OF $d = \Omega^2\Delta$ FOR SUBCASES IN THE SUMMARIES OF THEOREM 1 18

III. EXISTENCE OF PRIMITIVE, PROPERLY PRIMITIVE AND IMPROPERLY PRIMITIVE FORMS 31

IV. EXISTENCE OF FORMS IN WHICH $2^n||c_1$ AND EXISTENCE OF FORMS IN WHICH Ω DIVIDES THE COFACTORS OF THE ELEMENTS OF d 88

BIBLIOGRAPHY 128

BIOGRAPHICAL SKETCH 129

CHAPTER I

INTRODUCTION

All letters designate integers throughout this dissertation. A homogeneous quadratic polynomial in three variables, $ax^2 + by^2 + cz^2 + 2ryz + 2sxz + 2txy$ is called a ternary quadratic form and is denoted by f. A determinant

$$d = \begin{vmatrix} a & t & s \\ t & b & r \\ s & r & c \end{vmatrix}$$

is associated with a form f. A form f is said to be primitive if $(a, b, c, r, s, t) = 1$. A primitive form is said to be properly primitive or improperly primitive according as (a, b, c) is odd or even. Two forms are said to be equivalent if there is a linear transformation of determinant 1 which takes one form into the other. Equivalent forms have the same determinant associated with them.

Professor B.W. Jones [1] has proved that a form f is equivalent to one in which $t = 0$ and thus the form $f = ax^2 + by^2 + cz^2 + 2ryz + 2sxz$ of this dissertation is a general one.

Professor E.H. Hadlock's theorem [2], which is basic to this dissertation, is given below, in which he has proved the existence of a form $f = ax^2 + by^2 + cz^2 + 2ryz + 2sxz$ having the given determinant d associated with it.

Theorem 1: Let d and a be arbitrary positive integers, except let a factor a_2 of a be restricted as in (1.5) I_{21}. Let Ω^2 be any square divisor of d, thus defining the integer Δ by $\Omega^2\Delta = d$. Define Ω_1, Δ_1, a_1, b_1 and b by

$$\tag{1.1} \begin{cases} \Omega = 2^{\epsilon_1}\Omega_1, \quad \Delta = 2^{\epsilon_2}\Delta_1, \quad a = 2^{\epsilon_3}a_1, \\ b_1 = 2^{\epsilon_4}b_2, \quad b = \Omega b_1, \end{cases}$$

where 2^{ϵ_i}, $i = 1, 2, 3, 4$ are the highest powers of 2 dividing Ω, Δ, a and b_1 respectively, ϵ_4 is determined from the summaries of subcases which arise and b_2 is chosen to satisfy (1.3) - (1.5). Define δ_1, D, a_2, δ_2, Ω_2, Ω_3, D_1 and D_2 by

$$\tag{1.2} \begin{cases} \delta_1 = \Omega_1\Delta_1, \quad D = (a_1, \delta_1), \quad a_1 = Da_2, \\ \delta_1 = D\delta_2, \quad \Omega_1 = \Omega_2^2\Omega_3, \quad D = D_1^2 D_2, \end{cases}$$

where Ω_2^2 and D_1^2 are the largest squares dividing Ω_1 and D respectively. Take b_2 so that

$$\tag{1.3} (b_2, \delta_1 a_2) = 1,$$

and where

$$\tag{1.4} \begin{cases} (b_2|p) = (-2^h\delta_2 D_2|p), \quad h = h_2 + h_3 \\ (q|\delta_2\Omega_3 a_2) = (-1)^{(q-1)/2 \cdot (\delta_2\Omega_3 a_2 + 1)/2}(2^k|q), \\ \qquad k = h_1 + h_3 + k_1 + k_3, \end{cases}$$

for each prime factor p of a_2 and q of b_2 and where $h_i \geq 0$, $k_j \geq 0$, i, j = 1, 2, 3 are given in the summaries (i) - (iv) which follow.

(1.5)

If $h_1 > 1$, $h_2 = h_3 = 0$, then b_2 must satisfy

$$b_2D_2\alpha \equiv 1 \pmod{2^{h_1}}, \quad \alpha \equiv \begin{cases} 3\delta_2 \pmod{4} & \text{if } h_1 = 2 \\ 7\delta_2 \pmod{8} & \text{if } h_1 \geq 3 \end{cases}.$$

If I: $k_1 = k_3 = 0$, $k_2 > 1$, define $k' = \begin{cases} 2 & \text{if } k_2 = 2 \\ 3 & \text{if } k_2 \geq 3 \end{cases}$.

If I and I_1: $h_1 > 0$, $h_2 = h_3 = 0$, choose γ and b_2 to satisfy $\gamma \equiv 2^{h_1}7\Omega_3a_2 - \delta_2 \pmod{8}$ and $b_2D_2\gamma \equiv 1 \pmod{2^{h_1+k'}}$ respectively.

If I, I_2: $h_1 = h_3 = 0$, $h_2 \geq 0$ and if I_{21}: $2^{h_2}s_1 \equiv 0 \pmod{2}$, then a_2 is restricted by $a_2 \equiv 7\Omega_3(2^{h_2}b_2D_2s_1^2 + \delta_2) \pmod{2^{k'}}$.

If I, I_2 and I_{22}: $2^{h_2}s_1 \equiv 1 \pmod{2}$, iff $k_2 \geq 4$, choose γ and b_2 to satisfy $\gamma \equiv 4 - \delta_2 \pmod{8}$ and $b_2D_2\gamma \equiv 1 \pmod{2^{k'+2}}$ respectively.

If I and I_3: $h_1 = h_2 = 0$, $h_3 > 0$, then choose b_2 to satisfy $b_2 \equiv D_2(7\Omega_3a_2 - 2^{h_3}\delta_2) \pmod{2^{k'}}$.

(1.5) Finally, s_1 must be replaced by s_2 or s_3 if such occurs in (i) - (iv).

Then there exists a form $f = ax^2 + by^2 + cz^2 + 2ryz + 2sxz$ having the given determinant d associated with it.

In the following reproduction of the summaries of cases (i) - (iv) of theorem 1, a few subcases have been renumbered and a few changes have been made in notations for convenience.

Summaries of cases (i) - (iv) of theorem 1 follow for which the two equations

$$(1.6) \quad \begin{cases} 2^{h_1}a_2A_m - 2^{h_2}b_2D_2s_i^2 = 2^{h_3}\delta_2, \\ 2^{k_1}A_m = 2^{k_2}b_2c_1 - 2^{k_3}\Omega_3r_j^2 \end{cases}$$

hold simultaneously for one value of m = 1, 2, 3, one value of i = 1, 2, 3 and one value of j = 1, 2 to be determined from the summaries and in which at least two of h_1, h_2 and h_3 are zero and at least two of k_1, k_2 and k_3 are zero. Further, if the values of h_i, k_j, i, j = 1, 2, 3 are not listed, then their values are assumed to be zero. Recall that ε_1, ε_2, ε_3 and ε_4 are the exponents of the highest powers of 2 dividing Ω, Δ, a and b_1 respectively and that ε' and ε_5 are defined by $\varepsilon' = \varepsilon_1 + \varepsilon_2$ and $\varepsilon_5 = \varepsilon' - \varepsilon_3$. If (1.6) implies that s_i, A_m and r_j are odd, then they are so stated in the summaries. If $h_1 = h_2 = 0$ and $h_3 > 0$, then A_m is odd by choice of $s_i \equiv 1 \pmod 2$. Conditions on the parity of s_i, A_m and r_j due to $k_2 > 1$ do not necessarily hold if $k_2 = 1$.

Summary of subcases of (i) $\epsilon_3 \le \epsilon' \le \epsilon_4$:

$$(\mathrm{i})_1 \quad \begin{cases} \underline{\epsilon_2 < \epsilon_3,\ \epsilon_1 < \epsilon_4 = \epsilon'},\ h_1 = \epsilon_3 - \epsilon_2,\ k_2 = \epsilon_4 - \epsilon_1, \\ A = 2^{\epsilon_1}A_2,\ s_1A_2r_1 \text{ odd, } c \equiv 0 \text{ or } 1 \pmod 2 \\ \text{according as } r_1 \text{ satisfies } \Omega_3 r_1^2 + A_2 \equiv 0 \text{ or} \\ 2^{\epsilon_4-\epsilon_1} \pmod{2^{\epsilon_4-\epsilon_1+1}}. \end{cases}$$

$$(\mathrm{i})_2 \quad \begin{cases} \underline{\epsilon_2 = \epsilon_3,\ \epsilon_1 < \epsilon_4},\ h_2 = \epsilon_4 - \epsilon',\ k_2 = \epsilon_4 - \epsilon_1, \\ A = 2^{\epsilon_5}A_1,\ A_1r_1 \text{ odd if } \epsilon_4 > \epsilon';\ \text{ if } \epsilon_4 = \epsilon', \text{ then} \\ A_1r_1 \equiv s_1 + 1 \equiv 1 \pmod 2 \text{ or } (A_1/4)(r_1/2)s_1 \equiv 1 \pmod 2; \\ c \equiv 0 \text{ or } 1 \pmod 2 \text{ according as } r_1 \text{ satisfies} \\ \Omega_3 r_1^2 + A_1 \equiv 0 \text{ or } 2^{\epsilon_4-\epsilon_1} \pmod{2^{\epsilon_4-\epsilon_1+1}}. \end{cases}$$

$$(\mathrm{i})_3 \quad \begin{cases} \underline{0 = \epsilon_2 < \epsilon_3,\ \epsilon_1 = \epsilon_4},\ h_1 = \epsilon_3,\ A = 2^{\epsilon_1}A_2,\ s_1 \text{ odd,} \\ A_2 \equiv 0 \text{ or } 1 \pmod 2 \text{ according as } s_1 \text{ is chosen to} \\ \text{satisfy } b_2D_2s_1^2 + \delta_2 \equiv 0 \text{ or } 2^{\epsilon_3} \pmod{2^{\epsilon_3+1}}, \\ c \equiv A_2 + r_1 \pmod 2. \end{cases}$$

$$(\mathrm{i})_4 \quad \begin{cases} \underline{0 = \epsilon_2 = \epsilon_3,\ \epsilon_1 = \epsilon_4},\ A = 2^{\epsilon_1}A_1,\ A_1 \equiv s_1 + 1 \pmod 2, \\ c \equiv r_1 + s_1 + 1 \pmod 2. \end{cases}$$

$(\mathrm{i})_{51}$
$\underline{\epsilon_3 < \epsilon_2,\ \epsilon_5 < \epsilon_4,\ \epsilon_3 \equiv \epsilon_2 \pmod 2}$, $h_2 = \epsilon_4 - \epsilon'$,
$k_2 = \epsilon_4 - \epsilon_5$, $A = 2^{\epsilon_5}A_1$, $r_1 = 2^{(\epsilon_2-\epsilon_3)/2}r_2$,
A_1r_2 odd if $\epsilon_4 > \epsilon'$; $A_1r_2 \equiv s_1 + 1 \equiv 1 \pmod 2$ or
$(A_1/4)(r_2/2)s_1 \equiv 1 \pmod 2$ if $\epsilon_4 = \epsilon'$; $c \equiv 0$ or 1
$\pmod 2$ according as r_2 satisfies $\Omega_3r_2^2 + A_1 \equiv 0$ or
$2^{\epsilon_4-\epsilon_5} \pmod{2^{\epsilon_4-\epsilon_5+1}}$.

$(\mathrm{i})_{52}$
$\underline{0 < \epsilon_3 < \epsilon_2,\ \epsilon_4 = \epsilon',\ \epsilon_3 \equiv \epsilon_2 + 1 \pmod 2}$, $h_1 = 1$,
$k_2 = \epsilon_3 - 1$, $A = 2^{\epsilon_5+1}A_2$, $r_1 = 2^{(\epsilon_2-\epsilon_3+1)/2}r_2$,
s_1 odd, $c \equiv 0$ or $1 \pmod 2$ according as r_2
satisfies $\Omega_3r_2^2 + A_2 \equiv 0$ or $2^{\epsilon_3-1} \pmod{2^{\epsilon_3}}$.

$(\mathrm{i})_{61}$
$\underline{0 = \epsilon_3 < \epsilon_2,\ \epsilon' = \epsilon_4,\ \epsilon_2 \equiv 0 \pmod 2}$, $A = 2^{\epsilon_5}A_1$,
$r_1 = 2^{\epsilon_2/2}r_2$, $A_1 \equiv s_1 + 1 \pmod 2$,
$c \equiv s_1 + r_2 + 1 \pmod 2$.

$(\mathrm{i})_{62}$
$\underline{0 = \epsilon_3 < \epsilon_2,\ \epsilon' = \epsilon_4,\ \epsilon_2 \equiv 1 \pmod 2}$, $k_3 = 1$,
$A = 2^{\epsilon_5}A_1$, $r_1 = 2^{(\epsilon_2+1)/2}r_2$, $c \equiv A_1 \equiv s_1 + 1 \pmod 2$.

$(\mathrm{i})_7$, $(\mathrm{i})_8$: $\underline{\epsilon_1 \le \epsilon_4 < \epsilon_5 \text{ impossible.}}$

$\underline{\text{Summary of subcases of (ii)}\ \ \epsilon_4 \le \epsilon' \le \epsilon_3,\ \epsilon_4 \ne \epsilon_3,}$

$\underline{s_1 = 2^{[(\epsilon'-\epsilon_4+1)/2]} s_2:}$

$$(\text{ii})_{13} \left\{ \begin{array}{l} \underline{\epsilon_4 \le \epsilon_1,\ \epsilon_4 \equiv \epsilon' \pmod{2}},\ h_1 = \epsilon_4 - \epsilon_5,\ k_3 = \epsilon_1 - \epsilon_4, \\ A = 2^{\epsilon_4}A_1,\ S_2 \text{ odd if } \epsilon_5 < \epsilon_4,\ A_1 \equiv 0 \text{ or } 1 \pmod{2} \\ \text{according as } s_2 \text{ is chosen to satisfy} \\ b_2D_2s_2^2 + \delta_2 \equiv 0 \text{ or } 2^{\epsilon_4-\epsilon_5} \pmod{2^{\epsilon_4-\epsilon_5+1}}, \\ c \equiv A_1 + 2^{\epsilon_1-\epsilon_4}r_1 \pmod{2}. \end{array} \right.$$

$$(\text{ii})_{14} \left\{ \begin{array}{l} \underline{\epsilon_4 > \epsilon_1,\ \epsilon_4 \equiv \epsilon' \pmod{2}},\ h_1 = \epsilon_3 - \epsilon_2,\ k_2 = \epsilon_4 - \epsilon_1, \\ A = 2^{\epsilon_1}A_1,\ s_2A_1r_1 \text{ odd if } \epsilon_2 < \epsilon_3;\ A_1r_1 \equiv s_2 + 1 \equiv 1 \\ \pmod{2} \text{ or } (A_1/4)(r_1/2)s_2 \equiv 1 \pmod{2} \text{ if } \epsilon_2 = \epsilon_3; \\ c \equiv 0 \text{ or } 1 \pmod{2} \text{ according as } r_1 \text{ satisfies} \\ \Omega_3r_1^2 + A_1 \equiv 0 \text{ or } 2^{\epsilon_4-\epsilon_1} \pmod{2^{\epsilon_4-\epsilon_1+1}}. \end{array} \right.$$

$$(\text{ii})_{23} \left\{ \begin{array}{l} \underline{0 = \epsilon_4 \equiv \epsilon' + 1 \pmod{2},\ \epsilon_3 = \epsilon'},\ h_2 = 1,\ k_3 = \epsilon_1, \\ A \text{ odd, } c \equiv r_1 + 1 \text{ or } 1 \pmod{2} \text{ according as} \\ \epsilon_1 = 0 \text{ or } \epsilon_1 > 0. \end{array} \right.$$

$$(\mathrm{ii})_{24}\ \left\{\begin{array}{l}\underline{\varepsilon_1 = 0 < \varepsilon_4 \equiv \varepsilon_2 + 1 \pmod 2,\ \varepsilon_3 = \varepsilon_2},\ \ h_2 = 1,\\ k_2 = \varepsilon_4,\ Ar_1 \text{ odd, } c \equiv 0 \text{ or } 1 \pmod 2 \text{ according}\\ \text{as } r_1 \text{ satisfies } \Omega_3 r_1^2 + A \equiv 0 \text{ or } 2^{\varepsilon_4} \pmod{2^{\varepsilon_4+1}}.\end{array}\right.$$

Summary of subcases of (iii) $\varepsilon_3 \le \varepsilon_4 < \varepsilon'$:

$$(\mathrm{iii})_{111}\left\{\begin{array}{l}\underline{\varepsilon_4 \le \varepsilon_1,\ \varepsilon_4 \le \varepsilon_5,\ \varepsilon_3 \equiv 0 \pmod 2},\ h_3 = \varepsilon_5 - \varepsilon_4,\\ k_3 = \varepsilon_1 - \varepsilon_4,\ A = 2^{\varepsilon_4}A_2,\ s_1 = 2^{\varepsilon_3/2}s_2,\\ A_2 \equiv s_2 + 2^{\varepsilon_5-\varepsilon_4} \pmod 2,\ c \equiv A_2 + 2^{\varepsilon_1-\varepsilon_4}r_1 \pmod 2.\end{array}\right.$$

$$(\mathrm{iii})_{112}\left\{\begin{array}{l}\underline{\varepsilon_4 \le \varepsilon_1,\ \varepsilon_4 = \varepsilon_5,\ \varepsilon_3 \equiv 1 \pmod 2},\ h_2 = 1,\\ k_3 = \varepsilon_1 - \varepsilon_4,\ A = 2^{\varepsilon_4}A_2,\ A_2 \text{ odd, } s_1 = 2^{(\varepsilon_3+1)/2}s_2,\\ c \equiv 1 + 2^{\varepsilon_1-\varepsilon_4}r_1 \pmod 2.\end{array}\right.$$

$$(\mathrm{iii})_{121}\left\{\begin{array}{l}\underline{\varepsilon_4 \le \varepsilon_1,\ \varepsilon_4 > \varepsilon_5,\ \varepsilon_4 \equiv \varepsilon' \pmod 2},\ h_1 = \varepsilon_4 - \varepsilon_5,\\ k_3 = \varepsilon_1 - \varepsilon_4,\ A = 2^{\varepsilon_4}A_2,\ s_1 = 2^{(\varepsilon'-\varepsilon_4)/2}s_2,\\ s_2 \text{ odd, } A_2 \equiv 0 \text{ or } 1 \pmod 2 \text{ according as } s_2\\ \text{satisfies } b_2D_2s_2^2 + \delta_2 \equiv 0 \text{ or } 2^{\varepsilon_4-\varepsilon_5} \pmod{2^{\varepsilon_4-\varepsilon_5+1}},\\ c \equiv A_2 + 2^{\varepsilon_1-\varepsilon_4}r_1 \pmod 2.\end{array}\right.$$

$(\mathrm{iii})_{122}$: $\underline{\varepsilon_4 \le \varepsilon_1,\ \varepsilon_4 > \varepsilon_5,\ \varepsilon_4 \equiv \varepsilon' + 1 \pmod 2 \ \ \text{impossible}}$.

$(\text{iii})_{211}$

$\epsilon_1 < \epsilon_4 - \epsilon_3 < \epsilon_4$, $\epsilon_4 \equiv \epsilon_1 + \epsilon_3 \pmod{2}$,
$h_3 = \epsilon' - \epsilon_4$, $k_2 = \epsilon_3$, $A = 2^{\epsilon_4 - \epsilon_3}A_1$,
$r_1 = 2^{(\epsilon_4 - \epsilon_1 - \epsilon_3)/2} r_2$, $A \equiv s_1 \pmod{2}$; if $\epsilon_3 \geq 1$,
then $A_1 \equiv s_1 \equiv 1 \pmod{2}$; $c \equiv 0$ or $1 \pmod{2}$
according as r_2 satisfies $\Omega_3 r_2^2 + A_1 \equiv 0$ or
$2^{\epsilon_3} \pmod{2^{\epsilon_3 + 1}}$.

$(\text{iii})^*_{212}$

$\epsilon_3 < \epsilon_4 < \epsilon'$, $\epsilon_1 < \epsilon_4 - \epsilon_3 < \epsilon_4$, $\epsilon_4 \equiv \epsilon_1 + \epsilon_3 + 1$
$\pmod{2}$.

$(\text{iii})_{2211}$

$\epsilon_4 - \epsilon_3 \leq \epsilon_1 < \epsilon_4$, $\epsilon_3 > \epsilon_2$, $\epsilon_4 \equiv \epsilon' \pmod{2}$,
$h_1 = \epsilon_3 - \epsilon_2$, $k_2 = \epsilon_4 - \epsilon_1$, $A = 2^{\epsilon_1}A_2$,
$s_1 = 2^{(\epsilon' - \epsilon_4)/2} s_2$, $s_2 A_2 r_1$ odd, $c \equiv 0$ or $1 \pmod{2}$
according as r_1 satisfies $\Omega_3 r_1^2 + A_2 \equiv 0$ or
$2^{\epsilon_4 - \epsilon_1} \pmod{2^{\epsilon_4 - \epsilon_1 + 1}}$.

$(\text{iii})_{2212}$

$\epsilon_4 - \epsilon_3 \leq \epsilon_1 < \epsilon_4$, $\epsilon_3 > \epsilon_2$, $\epsilon_4 \equiv \epsilon' + 1 \pmod{2}$
impossible.

$(\text{iii})_{2221}$

$\underline{\epsilon_4 - \epsilon_3 \le \epsilon_1 < \epsilon_4,\ \epsilon_3 \le \epsilon_2,\ \epsilon_4 \equiv \epsilon_1 + \epsilon_3 \ (\text{mod } 2),}$
$h_3 = \epsilon_2 - \epsilon_3$, $k_2 = \epsilon_4 - \epsilon_1$, $A = 2^{\epsilon_1}A_2$,
$s_1 = 2^{(\epsilon_1 - \epsilon_4 + \epsilon_3)/2} s_2$, $A_2 s_2 r_1$ odd if $\epsilon_3 < \epsilon_2$;
if $\epsilon_3 = \epsilon_2$, then $A_2 r_1 \equiv s_2 + 1 \equiv 1 \ (\text{mod } 2)$ or
$(A_2/4)(r_1/2)s_2 \equiv 1 \ (\text{mod } 2)$; $c \equiv 0$ or $1 \ (\text{mod } 2)$
according as r_1 satisfies $\Omega_3 r_1^2 + A_2 \equiv 0$ or
$2^{\epsilon_4 - \epsilon_1} \ (\text{mod } 2^{\epsilon_4 - \epsilon_1 + 1})$.

$(\text{iii})_{2222}$

$\underline{\epsilon_4 - \epsilon_3 \le \epsilon_1 < \epsilon_4,\ \epsilon_3 = \epsilon_2,\ \epsilon_4 \equiv \epsilon_1 + \epsilon_3 + 1}$
$\underline{(\text{mod } 2)}$, $h_2 = 1$, $k_2 = \epsilon_4 - \epsilon_1$, $A = 2^{\epsilon_1}A_2$,
$s_1 = 2^{(\epsilon_1 - \epsilon_4 + \epsilon_3 + 1)/2} s_2$, $A_2 r_1 \equiv 1 \ (\text{mod } 2)$, $c \equiv 0$
or $1 \ (\text{mod } 2)$ according as r_1 satisfies
$\Omega_3 r_1^2 + A_2 \equiv 0$ or $2^{\epsilon_4 - \epsilon_1} \ (\text{mod } 2^{\epsilon_4 - \epsilon_1 + 1})$.

$(\text{iii})^{*}_{2223}$

$\underline{\epsilon_3 \le \epsilon_4 < \epsilon',\ \epsilon_4 - \epsilon_3 \le \epsilon_1 < \epsilon_4,\ \epsilon_3 < \epsilon_2,}$
$\underline{\epsilon_4 \equiv \epsilon_1 + \epsilon_3 + 1 \ (\text{mod } 2).}$

Summary of subcases of (iv) $\epsilon_4 < \epsilon_3 < \epsilon'$:

$$(\mathrm{iv})_{1311}\ \left\{\begin{array}{l} \underline{\epsilon_4 \le \epsilon_1,\ \epsilon_4 \equiv \epsilon_3 \pmod{2},\ \epsilon_4 \ge \epsilon_5,\ \epsilon_5 \equiv 0 \pmod{2},} \\ h_1 = \epsilon_4 - \epsilon_5,\ k_3 = \epsilon_1 - \epsilon_4,\ A = 2^{\epsilon_4}A_1, \\ s_1 = 2^{(\epsilon' - \epsilon_4)/2}s_3,\ A_1 \equiv 0 \text{ or } 1 \pmod{2} \text{ according} \\ \text{as } s_3 \text{ is chosen to satisfy } b_2D_2s_3^2 + \delta_2 \equiv 0 \text{ or} \\ 2^{\epsilon_4-\epsilon_5} \pmod{2^{\epsilon_4-\epsilon_5+1}},\ c \equiv A_1 + 2^{\epsilon_1-\epsilon_4}r_1 \pmod{2}. \end{array}\right.$$

$$(\mathrm{iv})_{1312}\ \left\{\begin{array}{l} \underline{\epsilon_4 \le \epsilon_1,\ \epsilon_4 \equiv \epsilon_3 \pmod{2},\ \epsilon_4 = \epsilon_5,\ \epsilon_5 \equiv 1 \pmod{2},} \\ h_2 = 1,\ k_3 = \epsilon_3 - \epsilon_2,\ A = 2^{\epsilon_4}A_1,\ s_1 = 2^{(\epsilon_3+1)/2}s_3, \\ A_1 \text{ odd},\ c \equiv 1 + 2^{\epsilon_3-\epsilon_2}r_1 \pmod{2}. \end{array}\right.$$

$$(\mathrm{iv})_{1321}\ \left\{\begin{array}{l} \underline{\epsilon_4 \le \epsilon_1,\ 0 \equiv \epsilon_4 \equiv \epsilon_3 \pmod{2},\ \epsilon_4 < \epsilon_5,} \\ h_3 = \epsilon_5 - \epsilon_4,\ k_3 = \epsilon_1 - \epsilon_4,\ A = 2^{\epsilon_4}A_1, \\ s_1 = 2^{\epsilon_3/2}s_3,\ A_1 \equiv s_3 \equiv 1 \pmod{2}, \\ c \equiv 1 + 2^{\epsilon_1-\epsilon_4}r_1 \pmod{2}. \end{array}\right.$$

$$(\mathrm{iv})_{13221}\ \left\{\begin{array}{l} \underline{\epsilon_4 = \epsilon_1,\ 1 \equiv \epsilon_4 \equiv \epsilon_3 \pmod{2},\ \epsilon_4 < \epsilon_5,} \\ h_3 = (\epsilon_5 - 1) - \epsilon_4,\ k_1 = 1, A = 2^{\epsilon_4+1}A_2, \\ s_1 = 2^{(\epsilon_3+1)/2}s_3,\ A_2 \equiv s_3 + 2^{(\epsilon_5-1)-\epsilon_4} \pmod{2}, \\ c \equiv r_1 \pmod{2}. \end{array}\right.$$

$$(\text{iv})_{13222}\begin{cases} \underline{\epsilon_4 < \epsilon_1,\ 1 \equiv \epsilon_4 \equiv \epsilon_3 \ (\text{mod } 2),\ \epsilon_4 < \epsilon_5,} \\ h_3 = (\epsilon_5 - 1) - \epsilon_4,\ k_3 = (\epsilon_1 - 1) - \epsilon_4, \\ A = 2^{\epsilon_4+1}A_2,\ s_1 = 2^{(\epsilon_3+1)/2}s_3,\ A_2 \equiv s_3 + 2^{(\epsilon_5-1)-\epsilon_4} \\ (\text{mod } 2),\ c = 2c_1,\ c_1 \equiv A_2 + 2^{(\epsilon_1-1)-\epsilon_4}r_1 \ (\text{mod } 2). \end{cases}$$

$$(\text{iv})_{1411}\begin{cases} \underline{\epsilon_4 \leq \epsilon_1,\ \epsilon_4 \equiv \epsilon_3 + 1 \ (\text{mod } 2),\ 1 \leq \epsilon_5 \leq \epsilon_4,} \\ \underline{\epsilon_5 \equiv 1 \ (\text{mod } 2),}\ h_1 = \epsilon_4 - \epsilon_5,\ k_3 = \epsilon_1 - \epsilon_4, \\ A = 2^{\epsilon_4}A_2,\ s_1 = 2^{(\epsilon' - \epsilon_4)/2}s_3,\ s_3 \text{ odd if } \epsilon_5 < \epsilon_4, \\ A_2 \equiv 0 \text{ or } 1 \ (\text{mod } 2) \text{ according as } s_3 \text{ satisfies} \\ b_2D_2s_3^2 + \delta_2 \equiv 0 \text{ or } 2^{\epsilon_4-\epsilon_5} (\text{mod } 2^{\epsilon_4-\epsilon_5+1}), \\ c \equiv A_2 + 2^{\epsilon_1-\epsilon_4}r_1 \ (\text{mod } 2). \end{cases}$$

$$(\text{iv})_{1412}\begin{cases} \underline{\epsilon_4 \leq \epsilon_1,\ \epsilon_4 \equiv \epsilon_3 + 1 \ (\text{mod } 2),\ 1 \leq \epsilon_5 = \epsilon_4,} \\ \underline{\epsilon_5 \equiv 0 \ (\text{mod } 2),}\ h_2 = 1,\ k_3 = \epsilon_1 - \epsilon_4,\ A = 2^{\epsilon_4}A_2, \\ s_1 = 2^{(\epsilon' - \epsilon_4 + 1)/2}s_3,\ A_2 \text{ odd},\ c \equiv 1 + 2^{\epsilon_1-\epsilon_4}r_1 \ (\text{mod } 2). \end{cases}$$

$$(\text{iv})_{1421}\begin{cases} \underline{\epsilon_4 \leq \epsilon_1,\ 1 \leq \epsilon_4 < \epsilon_5,\ 1 \equiv \epsilon_4 \equiv \epsilon_3 + 1 \ (\text{mod } 2),} \\ h_3 = \epsilon_5 - \epsilon_4,\ k_3 = \epsilon_1 - \epsilon_4,\ A = 2^{\epsilon_4}A_2,\ s_1 = 2^{\epsilon_3/2}s_3, \\ A_2s_3 \text{ odd},\ c \equiv 1 + 2^{\epsilon_1-\epsilon_4}r_1 \ (\text{mod } 2). \end{cases}$$

$$(\mathrm{iv})_{14221}\begin{cases}\underline{\varepsilon_4 = \varepsilon_1,\ 1 \le \varepsilon_4 < \varepsilon_5,\ 0 \equiv \varepsilon_4 \equiv \varepsilon_3 + 1 \pmod 2,}\\[1ex] h_3 = (\varepsilon_5 - 1) - \varepsilon_4,\ k_1 = 1,\ A = 2^{\varepsilon_4+1}A_3,\\[1ex] s_1 = 2^{(\varepsilon_3+1)/2}s_3,\ A_3 \equiv s_3 + 2^{(\varepsilon_5-1)-\varepsilon_4} \pmod 2,\\[1ex] c \equiv r_1 \pmod 2.\end{cases}$$

$$(\mathrm{iv})_{14222}\begin{cases}\underline{\varepsilon_4 < \varepsilon_1,\ 1 \le \varepsilon_4 < \varepsilon_5,\ 0 \equiv \varepsilon_4 \equiv \varepsilon_3 + 1 \pmod 2,}\\[1ex] h_3 = (\varepsilon_5 - 1) - \varepsilon_4,\ k_3 = (\varepsilon_1 - 1) - \varepsilon_4,\\[1ex] A = 2^{\varepsilon_4+1}A_3,\ s_1 = 2^{(\varepsilon_3+1)/2}s_3,\ A_3 \equiv s_3 + 2^{(\varepsilon_5-1)-\varepsilon_4}\\[1ex] \pmod 2,\ c = 2c_1,\ c_1 \equiv A_3 + 2^{(\varepsilon_1-1)-\varepsilon_4}r_1 \pmod 2.\end{cases}$$

$$(\mathrm{iv})_{2311}\begin{cases}\underline{\varepsilon_4 > \varepsilon_1,\ \varepsilon_4 \equiv \varepsilon_3 \pmod 2,\ \varepsilon_3 \ge \varepsilon_2,\ \varepsilon_5 \equiv 0 \pmod 2,}\\[1ex] h_1 = \varepsilon_3 - \varepsilon_2,\ k_2 = \varepsilon_4 - \varepsilon_1,\ A = 2^{\varepsilon_1}A_1,\\[1ex] s_1 = 2^{(\varepsilon' - \varepsilon_4)/2}s_3,\ s_3A_1r_1 \text{ odd if } \varepsilon_3 > \varepsilon_2;\\[1ex] A_1r_1 \equiv s_3 + 1 \equiv 1 \pmod 2 \text{ or } (A_1/4)(r_1/2)s_3 \equiv 1\\[1ex] \pmod 2 \text{ if } \varepsilon_3 = \varepsilon_2;\ c \equiv 0 \text{ or } 1 \pmod 2 \text{ according}\\[1ex] \text{as } r_1 \text{ satisfies } \Omega_3 r_1^2 + A_1 \equiv 0 \text{ or } 2^{\varepsilon_4-\varepsilon_1}\\[1ex] (\mathrm{mod}\ 2^{\varepsilon_4-\varepsilon_1+1}).\end{cases}$$

$(\mathrm{iv})_{2312}$
$\underline{\epsilon_4 > \epsilon_1,\ \epsilon_4 \equiv \epsilon_3 \ (\mathrm{mod}\ 2),\ \epsilon_3 = \epsilon_2,\ \epsilon_5 \equiv 1 \ (\mathrm{mod}\ 2),}$
$h_2 = 1,\ k_2 = \epsilon_4 - \epsilon_1,\ A = 2^{\epsilon_1}A_1,\ s_1 = 2^{(\epsilon' - \epsilon_4 + 1)/2}s_3,$
A_1r_1 odd, $c \equiv 0$ or 1 (mod 2) according as r_1
satisfies $\Omega_3 r_1^2 + A_1 \equiv 0$ or $2^{\epsilon_4 - \epsilon_1}$ (mod $2^{\epsilon_4 - \epsilon_1 + 1}$).

$(\mathrm{iv})_{2321}$
$\underline{\epsilon_4 > \epsilon_1,\ \epsilon_4 \equiv \epsilon_3 \ (\mathrm{mod}\ 2),\ \epsilon_3 < \epsilon_2,\ \epsilon_1 \equiv 0 \ (\mathrm{mod}\ 2),}$
$h_3 = \epsilon_2 - \epsilon_3,\ k_2 = \epsilon_4 - \epsilon_1,\ A = 2^{\epsilon_1}A_1,$
$s_1 = 2^{(\epsilon_1 + \epsilon_3 - \epsilon_4)/2}s_3,\ s_3A_1r_1$ odd, $c \equiv 0$ or 1
(mod 2) according as r_1 satisfies $\Omega_3 r_1^2 + A_1 \equiv 0$
or $2^{\epsilon_4 - \epsilon_1}$(mod $2^{\epsilon_4 - \epsilon_1 + 1}$).

$(\mathrm{iv})^*_{2322}$: $\underline{\epsilon_4 > \epsilon_1,\ \epsilon_4 \equiv \epsilon_3 \ (\mathrm{mod}\ 2),\ \epsilon_3 < \epsilon_2,\ \epsilon_1 \equiv 1 \ (\mathrm{mod}\ 2).}$

$(\mathrm{iv})_{2411}$
$\underline{\epsilon_4 > \epsilon_1 \geq 1,\ \epsilon_4 \equiv \epsilon_3 + 1 \ (\mathrm{mod}\ 2),\ \epsilon_3 \geq \epsilon_2,}$
$\underline{\epsilon_5 \equiv 1 \ (\mathrm{mod}\ 2),}\ h_1 = \epsilon_3 - \epsilon_2,\ k_2 = \epsilon_4 - \epsilon_1,$
$A = 2^{\epsilon_1}A_2,\ s_1 = 2^{(\epsilon' - \epsilon_4)/2}s_3,\ s_3A_2r_1$ odd if
$\epsilon_3 > \epsilon_2;\ A_2r_1 \equiv s_3 + 1 \equiv 1$ (mod 2) or
$(A_2/4)(r_1/2)s_3 \equiv 1$ (mod 2) if $\epsilon_3 = \epsilon_2$; $c \equiv 0$ or
1 (mod 2) according as r_1 satisfies $\Omega_3 r_1^2 + A_2 \equiv 0$
or $2^{\epsilon_4 - \epsilon_1}$ (mod $2^{\epsilon_4 - \epsilon_1 + 1}$).

$$(\mathrm{iv})_{24121}\begin{cases}\underline{\epsilon_4 > \epsilon_1 \ge 1,\ \epsilon_4 \equiv \epsilon_3 + 1 \pmod{2},\ \epsilon_3 > \epsilon_2,}\\[2ex] \underline{\epsilon_5 \equiv 0 \pmod{2}\text{ impossible.}}\end{cases}$$

$$(\mathrm{iv})_{24122}\begin{cases}\underline{\epsilon_4 > \epsilon_1 \ge 1,\ \epsilon_4 \equiv \epsilon_3 + 1 \pmod{2},\ \epsilon_3 = \epsilon_2,}\\[2ex] \underline{\epsilon_5 \equiv 0 \pmod{2}},\ h_2 = 1,\ k_2 = \epsilon_4 - \epsilon_1,\ A = 2^{\epsilon_1}A_2,\\[2ex] s_1 = 2^{(\epsilon'-\epsilon_4+1)/2}s_3,\ c \equiv 0 \text{ or } 1 \pmod{2} \text{ according}\\[2ex] \text{as } r_1 \text{ satisfies } \Omega_3 r_1^2 + A_2 \equiv 0 \text{ or } 2^{\epsilon_4-\epsilon_1} \pmod{2^{\epsilon_4-\epsilon_1+1}}.\end{cases}$$

$$(\mathrm{iv})^{*}_{2421}\begin{cases}\underline{\epsilon_4 > \epsilon_1 \ge 1,\ \epsilon_4 \equiv \epsilon_3 + 1 \pmod{2},\ \epsilon_3 < \epsilon_2,}\\[2ex] \underline{\epsilon_1 \equiv 0 \pmod{2}}.\end{cases}$$

$$(\mathrm{iv})_{2422}\begin{cases}\underline{\epsilon_4 > \epsilon_1 \ge 1,\ \epsilon_4 \equiv \epsilon_3 + 1 \pmod{2},\ \epsilon_3 < \epsilon_2,}\\[2ex] \underline{\epsilon_1 \equiv 1 \pmod{2}},\ h_3 = \epsilon_2 - \epsilon_3,\ k_2 = \epsilon_4 - \epsilon_1,\\[2ex] A = 2^{\epsilon_1}A_2,\ s_1 = 2^{(\epsilon_1+\epsilon_3-\epsilon_4)/2}s_3,\ s_3A_2r_1 \text{ odd},\\[2ex] c \equiv 0 \text{ or } 1 \pmod{2} \text{ according as } r_1 \text{ satisfies}\\[2ex] \Omega_3 r_1^2 + A_2 \equiv 0 \text{ or } 2^{\epsilon_4-\epsilon_1} \pmod{2^{\epsilon_4-\epsilon_1+1}}.\end{cases}$$

$$(\mathrm{iv})_{243}\begin{cases}\underline{\epsilon_4 > \epsilon_1,\ \epsilon_4 \equiv \epsilon_3 + 1 \pmod{2},\ \epsilon_1 = 0,\ \epsilon_4 = 1,}\\[2ex] \underline{\epsilon_3 \equiv 0 \pmod{2}},\ h_3 = \epsilon_2 - \epsilon_3 - 1,\ k_3 = 1,\ A = 2A_1,\\[2ex] s_1 = 2^{\epsilon_3/2}s_2,\ r_1 = 2r_2,\ c \equiv A_1s_2 \equiv 1 \pmod{2} \text{ by}\\[2ex] \text{choice of } s_2 \text{ if } \epsilon_2 > \epsilon_3 + 1 \text{ and } A_1 \equiv s_2 + 1 \equiv 1\\ \pmod{2} \text{ if } \epsilon_2 = \epsilon_3 + 1.\end{cases}$$

The four * cases $(iii)^*_{212}$, $(iii)^*_{2223}$, $(iv)^*_{2322}$ and $(iv)^*_{2421}$ are not discussed in this dissertation.

To construct a form, s, r and c are determined as follows:

From $(1.6)_1$, obtain

$$(1.7) \qquad 2^{h_2} b_2 D_2 s_i^2 \equiv -2^{h_3} \delta_2 \pmod{2^{h_1} a_2},$$

which yields s_i. Then A_m is found from $(1.6)_1$.
Now from $(1.6)_2$, obtain

$$(1.8) \qquad 2^{k_3} \Omega_3 r_j^2 \equiv -2^{k_1} A_m \pmod{2^{k_2} b_2},$$

which yields r_j. Then c_1 is found from $(1.6)_2$. Since s_1 is replaced by s_2 or s_3, r_1 by r_2 and c by c_1 in some subcases of theorem 1, define

$$(1.9) \qquad s_1 = 2^{m_1} s_i, \; i = 1, 2, 3;$$

$$(1.10) \qquad r_1 = 2^{m_2} r_j, \; j = 1, 2;$$

$$(1.11) \qquad c = 2^{m_3} c_1,$$

where m_1, m_2 and m_3 are determined from the summaries of theorem 1, for example, in the summary of subcase $(ii)_{23}$, no relation involving s_2 or s_3 occurs, which means there is no replacement of s_1, and thus i = 1 and $m_1 = 0$. In the summary of subcase $(iii)_{111}$, $s_1 = 2^{\varepsilon_3/2} s_2$, and thus i = 2 and $m_1 = \varepsilon_3/2$. In the summary of subcase $(iv)_{1321}$, $s_1 = 2^{\varepsilon_3/2} s_3$, and thus i = 3 and $m_1 = \varepsilon_3/2$. Similarly m_2 and m_3 are determined. Finally s and r are computed from the formulas

$$s = D_1 D_2 s_1 \tag{1.12}$$

and

$$r = 2^{\epsilon_1} \Omega_2 \Omega_3 r_1 \tag{1.13}$$

respectively.

CHAPTER II

FORMULAS FOR s_i, r_j AND c_1 AND VERIFICATION OF $d = \Omega^2\Delta$ FOR SUBCASES IN THE SUMMARIES OF THEOREM 1

Theorem 2: In the construction of a form $f = ax^2 + by^2 + cz^2 + 2ryz + 2sxz$, s_i, r_j and c_1 are given by

$$(2.1) \qquad s_i = 2^{h_1}a_2\beta \pm \lambda, \quad i = 1, 2, 3,$$

$$(2.2) \qquad r_j = 2^{k_2}b_2\rho \pm \mu, \quad j = 1, 2$$

and

$$(2.3) \quad \left\{ \begin{aligned} c_1 = c_1(\beta, \rho) = {} & 2^{h_1+h_2+k_1-k_2}a_2D_2\beta^2 + 2^{k_2+k_3}b_2\Omega_3\rho^2 \\ & \pm 2^{h_2+k_1-k_2+1}D_2\lambda\beta \pm 2^{k_3+1}\Omega_3\mu\rho \\ & + [2^{k_1}(2^{h_2}b_2D_2q_2 - 2^{h_3}\delta_2q_1) \\ & \quad + 2^{k_3}\Omega_3\mu^2]/2^{k_2}b_2, \end{aligned} \right.$$

where the signs in (2.1) and (2.2) agree with the signs of the coefficients of β and ρ respectively in (2.3); β is arbitrary if $h_2 \geq k_2$; if $h_2 < k_2$, then β is chosen to satisfy

$$(2.4) \qquad \beta(2^{h_1}a_2\beta \pm 2\lambda) \equiv 0 \pmod{2^{k_2-h_2}};$$

ρ is arbitrary; λ is the least positive residue mod $2^{h_1}a_2$

satisfying

(2.5) $$s_i^2 \equiv -2^{h_3}\delta_2\alpha \pmod{2^{h_1}a_2},$$

where α is defined by

(2.6) $$2^{h_2}b_2D_2\alpha \equiv 1 \pmod{2^{h_1}a_2};$$

μ is the least positive residue mod $2^{k_2}b_2$ satisfying

(2.7) $$r_j^2 \equiv -2^{k_1}A_m\gamma \pmod{2^{k_2}b_2}, \quad m = 1, 2, 3,$$

where A_m is given by

(2.8) $$A_m = 2^{h_2}b_2D_2[q_2 + \beta(2^{h_1}a_2\beta \pm 2\lambda)] - 2^{h_3}\delta_2q_1$$

and γ is defined by

(2.9) $$2^{k_3}\Omega_3\gamma \equiv 1 \pmod{2^{k_2}b_2};$$

q_1 is defined by

(2.10) $$q_1 = (2^{h_2}b_2D_2\alpha - 1)/2^{h_1}a_2$$

and q_2 is defined by

(2.11) $$q_2 = (\lambda^2 + 2^{h_3}\delta_2\alpha)/2^{h_1}a_2.$$

Proof: To prove (2.1), obtain from $(1.6)_1$,

(2.12) $$2^{h_2}b_2D_2s_i^2 \equiv -2^{h_3}\delta_2 \pmod{2^{h_1}a_2}.$$

From (2.6) and (2.12) obtain (2.5). Now (2.5) yields

(2.13) $$s_i \equiv \pm \lambda \pmod{2^{h_1}a_2},$$

which reduces to (2.1) when written as an equation.

To prove (2.2), obtain from $(1.6)_2$,

$$2^{k_3}\Omega_3 r_j^2 \equiv -2^{k_1}A_m \pmod{2^{k_2}b_2}. \tag{2.14}$$

From (2.9) and (2.14), obtain (2.7). From $(1.6)_1$, obtain

$$A_m = (2^{h_2}b_2D_2s_i^2 + 2^{h_3}\delta_2)/2^{h_1}a_2. \tag{2.15}$$

Now (2.1) and (2.15) yield

$$\left\{\begin{aligned} A_m = {} & 2^{h_2}b_2D_2\beta(2^{h_1}a_2\beta \pm 2\lambda) \\ & + (2^{h_2}b_2D_2\lambda^2 + 2^{h_3}\delta_2)/2^{h_1}a_2. \end{aligned}\right. \tag{2.16}$$

From (2.5) and (2.13), observe that $2^{h_1}a_2$ divides $(\lambda^2 + 2^{h_3}\delta_2\alpha)$, and thus define q_2 by (2.11). From (2.11) and (2.16), obtain

$$\left\{\begin{aligned} A_m = {} & 2^{h_2}b_2D_2\beta(2^{h_1}a_2\beta \pm 2\lambda) + 2^{h_2}b_2D_2q_2 \\ & - 2^{h_3}\delta_2(2^{h_2}b_2D_2\alpha - 1)/2^{h_1}a_2. \end{aligned}\right. \tag{2.17}$$

From (2.6), observe that $2^{h_1}a_2$ divides $(2^{h_2}b_2D_2\alpha - 1)$, and thus define q_1 by (2.10). Now (2.10) and (2.17) yield (2.8). It is seen from (2.8) that if $h_2 \geq k_2$, then β is arbitrary and

$$A_m \equiv -2^{h_3}\delta_2q_1 \pmod{2^{k_2}b_2}, \tag{2.18}$$

and if $h_2 < k_2$, then β is chosen to satisfy (2.4) and

$$A_m \equiv 2^{h_2}b_2D_2q_2 - 2^{h_3}\delta_2q_1 \pmod{2^{k_2}b_2}. \tag{2.19}$$

Using (2.18) or (2.19) according as $h_2 \geq k_2$ or $h_2 < k_2$ in (2.7), obtain

$$(2.20) \qquad r_j \equiv \pm \mu \pmod{2^{k_2} b_2},$$

which reduces to (2.2) when written as an equation.

To prove (2.3), obtain from $(1.6)_2$,

$$(2.21) \qquad c_1 = (2^{k_1} A_m + 2^{k_3} \Omega_3 r_j^2)/2^{k_2} b_2.$$

From (2.2), (2.8) and (2.21), obtain (2.3).

Finally, to show that c_1 in (2.3) is an integer, define c_2 and c_3 by

$$(2.22) \qquad c_2 = 2^{h_2+k_1} D_2 \beta (2^{h_1} a_2 \beta \pm 2\lambda)/2^{k_2},$$

and

$$(2.23) \qquad c_3 = [2^{k_1}(2^{h_2} b_2 D_2 q_2 - 2^{h_3} \delta_2 q_1) + 2^{k_3} \Omega_3 \mu^2]/2^{k_2} b_2.$$

Since ρ is arbitrary, it is sufficient to show that c_2 and c_3 are integers. Now to show that c_2 is an integer, observe from (2.22) that if $k_2 = 0$, then c_2 is an integer; if $k_2 > 0$, then $k_1 = 0$; further if $h_2 \geq k_2$, then c_2 is an integer; if $h_2 < k_2$, then β is chosen to satisfy (2.4), and thus c_2 is an integer in all cases. Next, to show that c_3 is an integer, obtain from (2.10), (2.11) and (2.23),

$$(2.24) \qquad \begin{cases} c_3 = [2^{k_1}(2^{h_2} b_2 D_2 \lambda^2 + 2^{h_3} \delta_2) \\ \qquad + 2^{h_1+k_3} a_2 \Omega_3 \mu^2]/2^{h_1+k_2} a_2 b_2. \end{cases}$$

It follows from (2.12) and (2.13) that $2^{h_1}a_2$ divides $(2^{h_2}b_2D_2\lambda^2 + 2^{h_3}\delta_2)$, and thus define q_3 by

$$(2.25) \qquad q_3 = (2^{h_2}b_2D_2\lambda^2 + 2^{h_3}\delta_2)/2^{h_1}a_2.$$

From (2.24) and (2.25), obtain

$$(2.26) \qquad c_3 = (2^{k_1}q_3 + 2^{k_3}\Omega_3\mu^2)/2^{k_2}b_2.$$

From (2.14) and (2.20), it follows that $2^{k_2}b_2$ divides $(2^{k_3}\Omega_3\mu^2 + 2^{k_1}A_m)$, and thus define q_4 by

$$(2.27) \qquad q_4 = (2^{k_3}\Omega_3\mu^2 + 2^{k_1}A_m)/2^{k_2}b_2.$$

Now (2.16), (2.22), (2.25) - (2.27) yield

$$(2.28) \qquad c_3 = q_4 - c_2,$$

which is an integer and the proof of the theorem is complete.

Corollary 2: c_1 in theorem 2 is also given by

$$(2.29) \qquad c_1 = 2^{k_3}\Omega_3\rho(2^{k_2}b_2\rho \pm 2\mu) + q_4,$$

where q_4 is defined by (2.27).

Proof: (2.3), (2.22), (2.24) and (2.28) yield (2.29).

Remark: In (2.4), the linear congruences

$$(2.30) \qquad 2^{h_1}a_2\beta \equiv \mp 2\lambda \pmod{2^{k_2-h_2}}$$

have no solutions or $(2^{h_1}, 2^{k_2-h_2})$ incongruent solutions according as $(2^{h_1}, 2^{k_2-h_2})$ is not or is a divisor of (2λ).

Verification of $d = \Omega^2\Lambda$ for subcases in the summaries of theorem 1:

By definition, $d = \begin{vmatrix} a & 0 & s \\ 0 & b & r \\ s & r & c \end{vmatrix}$,

which implies that

$$d = abc - ar^2 - bs^2. \tag{2.31}$$

From (1.1), (1.2), (1.9) - (1.13), (2.1), (2.2), (2.29) and (2.31), obtain

$$\begin{aligned} d = {} & 2^{\epsilon_3}Da_2 2^{\epsilon_1+\epsilon_4}\Omega_1 b_2 2^{m_3}[2^{k_3}\Omega_3\rho(2^{k_2}b_2\rho \pm 2\mu) + q_4] \\ & - 2^{\epsilon_3}Da_2 2^{2(\epsilon_1+m_2)}\Omega_2^2\Omega_3^2(2^{k_2}b_2\rho \pm \mu)^2 \\ & - 2^{\epsilon_1+\epsilon_4}\Omega_1 b_2 2^{2m_1}D_1^2D_2^2(2^{h_1}a_2\beta \pm \lambda)^2, \end{aligned}$$

which implies that

$$\left\{ \begin{aligned} d = {} & 2^{\epsilon_1}D\Omega_1[2^{\epsilon_3}(2^{\epsilon_4+k_3+m_3} - 2^{\epsilon_1+k_2+2m_2})(2^{k_2}b_2\rho \pm 2\mu) \\ & a_2b_2\Omega_3\rho + 2^{\epsilon_3+\epsilon_4+m_3}a_2b_2q_4 - 2^{\epsilon_1+\epsilon_3+2m_2}a_2\Omega_3\mu^2 \\ & - 2^{\epsilon_4+2h_1+2m_1}a_2^2b_2D_2\beta^2 \mp 2^{\epsilon_4+h_1+2m_1+1}a_2b_2D_2\lambda\beta \\ & - 2^{\epsilon_4+2m_1}b_2D_2\lambda^2]. \end{aligned} \right. \tag{2.32}$$

Now consider the second term of the right member of (2.32). Denote it by T_2 and write

$$T_2 = (2^{\epsilon_1}D\Omega_1)2^{\epsilon_3+\epsilon_4+m_3}a_2b_2q_4. \tag{2.33}$$

From (2.8), (2.27) and (2.33), obtain

$$\left\{\begin{aligned} T_2 = (2^{\epsilon_1}D\Omega_1)[&2^{\epsilon_3+\epsilon_4-k_2+k_3+m_3}a_2\Omega_3\mu^2 \\ &+ 2^{\epsilon_3+\epsilon_4+h_2+k_1-k_2+m_3}a_2b_2D_2q_2 \\ &+ 2^{\epsilon_3+\epsilon_4+h_1+h_2+k_1-k_2+m_3}a_2^2b_2D_2\beta^2 \\ &\pm 2^{\epsilon_3+\epsilon_4+h_2+k_1-k_2+m_3+1}a_2b_2D_2\lambda\beta \\ &- 2^{\epsilon_3+\epsilon_4+h_3+k_1-k_2+m_3}a_2\delta_2q_1]. \end{aligned}\right. \tag{2.34}$$

Now (2.32) and (2.34) yield

$$\left\{\begin{aligned} d = 2^{\epsilon_1}D\Omega_1[&2^{\epsilon_3}(2^{\epsilon_4+k_3+m_3} - 2^{\epsilon_1+k_2+2m_2})(2^{k_2}b_2\rho \pm 2\mu) \\ &a_2b_2\Omega_3\rho + 2^{\epsilon_3-k_2}(2^{\epsilon_4+k_3+m_3} - 2^{\epsilon_1+k_2+2m_2})a_2\Omega_3\mu^2 \\ &+ 2^{\epsilon_4+h_1}(2^{\epsilon_3+h_2+k_1-k_2+m_3} - 2^{h_1+2m_1})a_2^2b_2D_2\beta^2 \\ &\pm 2^{\epsilon_4+1}(2^{\epsilon_3+h_2+k_1-k_2+m_3} - 2^{h_1+2m_1})a_2b_2D_2\lambda\beta + N], \end{aligned}\right. \tag{2.35}$$

where N is given by

$$\left\{\begin{aligned} N = 2^{\epsilon_3+\epsilon_4-h_1+k_1-k_2+m_3}(&2^{h_1+h_2}a_2b_2D_2q_2 \\ &- 2^{h_1+h_3}a_2\delta_2q_1) - 2^{\epsilon_4+2m_1}b_2D_2\lambda^2. \end{aligned}\right. \tag{2.36}$$

From (2.10), (2.11) and (2.36), obtain

$$\left\{\begin{aligned} N = {}&2^{\epsilon_4-h_1}(2^{\epsilon_3+h_2+k_1-k_2+m_3} - 2^{h_1+2m_1})b_2D_2\lambda^2 \\ &+ 2^{\epsilon_3+\epsilon_4-h_1+h_3+k_1-k_2+m_3}\delta_2. \end{aligned}\right. \tag{2.37}$$

It follows from (2.35) and (2.37) that

$$(2.38)\quad \left\{ \begin{aligned} d = {} & 2^{\varepsilon_1} D\Omega_1 [2^{\varepsilon_3 - k_2}(2^{\varepsilon_4 + k_3 + m_3} - 2^{\varepsilon_1 + k_2 + 2m_2}) a_2 \Omega_3 \\ & \{2^{k_2} b_2 \rho (2^{k_2} b_2 \rho \pm 2\mu) + \mu^2\} \\ & + 2^{\varepsilon_4 - h_1}(2^{\varepsilon_3 + h_2 + k_1 - k_2 + m_3} - 2^{h_1 + 2m_1}) b_2 D_2 \\ & \{2^{h_1} a_2 \beta (2^{h_1} a_2 \beta \pm 2\lambda) + \lambda^2\} \\ & + 2^{\varepsilon_3 + \varepsilon_4 - h_1 + h_3 + k_1 - k_2 + m_3} \delta_2]. \end{aligned} \right.$$

Now for each subcase in the summaries of theorem 1, verify that

$$(2.39)\qquad \varepsilon_4 + k_3 + m_3 = \varepsilon_1 + k_2 + 2m_2,$$

$$(2.40)\qquad \varepsilon_3 + h_2 + k_1 - k_2 + m_3 = h_1 + 2m_1,$$

and

$$(2.41)\qquad \varepsilon_3 + \varepsilon_4 - h_1 + h_3 + k_1 - k_2 + m_3 = \varepsilon_1 + \varepsilon_2.$$

In subcases

$(i)_1$, $(i)_2$, $(i)_3$, $(i)_4$, $(i)_{51}$, $(i)_{52}$, $(i)_{61}$,
$(ii)_{14}$, $(ii)_{24}$, $(iii)_{211}$, $(iii)_{2211}$,
$(iii)_{2221}$, $(iii)_{2222}$, $(iv)_{13221}$, $(iv)_{14221}$,
$(iv)_{2311}$, $(iv)_{2312}$, $(iv)_{2321}$, $(iv)_{2411}$,
$(iv)_{24122}$ and $(iv)_{2422}$,

each member of (2.39) is equal to ε_4. In subcases $(i)_{62}$

and $(iv)_{243}$, each member of (2.39) is equal to $\varepsilon_4 + 1$. In subcases

$(ii)_{13}$, $(ii)_{23}$, $(iii)_{111}$, $(iii)_{112}$, $(iii)_{121}$,

$(iv)_{1311}$, $(iv)_{1312}$, $(iv)_{1321}$, $(iv)_{13222}$,

$(iv)_{1411}$, $(iv)_{1412}$, $(iv)_{1421}$ and $(iv)_{14222}$,

each member of (2.39) is equal to ε_1. Thus (2.39) is verified.

In subcase $(i)_1$, each member of (2.40) is equal to $\varepsilon_3 - \varepsilon_2$. In subcases $(i)_2$, $(i)_4$, $(i)_{51}$, $(i)_{61}$, $(i)_{62}$ and $(iii)_{211}$, each member of (2.40) is equal to zero. In subcases

$(i)_3$, $(ii)_{13}$, $(iii)_{111}$, $(iii)_{121}$, $(iv)_{1311}$,

$(iv)_{1321}$, $(iv)_{1411}$, $(iv)_{1421}$ and $(iv)_{243}$,

each member of (2.40) is equal to ε_3. In subcase $(i)_{52}$, each member of (2.40) is equal to 1. In subcases

$(ii)_{14}$, $(iii)_{2211}$, $(iii)_{2221}$, $(iv)_{2311}$,

$(iv)_{2321}$, $(iv)_{2411}$ and $(iv)_{2422}$,

each member of (2.40) is equal to $\varepsilon_1 + \varepsilon_3 - \varepsilon_4$. In subcases

$(ii)_{23}$, $(iii)_{112}$, $(iv)_{1312}$, $(iv)_{13221}$,

$(iv)_{13222}$, $(iv)_{1412}$, $(iv)_{14221}$ and $(iv)_{14222}$,

each member of (2.40) is equal to $\varepsilon_3 + 1$. In subcase $(ii)_{24}$, each member of (2.40) is equal to $\varepsilon_3 - \varepsilon_4 + 1$. In subcase

$(\mathrm{iii})_{2222}$, each member of (2.40) is equal to $\varepsilon_1 + \varepsilon_3 - \varepsilon_4 + 1$. Finally in subcases $(\mathrm{iv})_{2312}$ and $(\mathrm{iv})_{24122}$, each member of (2.40) is equal to $\varepsilon' - \varepsilon_4 + 1$. Thus (2.40) is verified.

Now (2.41) is verified as follows:

In $(\mathrm{i})_1$, $\varepsilon_3 + \varepsilon_4 - h_1 + h_3 + k_1 - k_2 + m_3 = \varepsilon_3 + \varepsilon_4 - (\varepsilon_3 - \varepsilon_2) + 0 + 0 - (\varepsilon_4 - \varepsilon_1) + 0 = \varepsilon_1 + \varepsilon_2$. In $(\mathrm{i})_2$, $\varepsilon_3 + \varepsilon_4 - h_1 + h_3 + k_1 - k_2 + m_3 = \varepsilon_3 + \varepsilon_4 - 0 + 0 + 0 - (\varepsilon_4 - \varepsilon_1) + 0 = \varepsilon_1 + \varepsilon_2$, since $\varepsilon_2 = \varepsilon_3$. In $(\mathrm{i})_3$, $\varepsilon_3 + \varepsilon_4 - h_1 + h_3 + k_1 - k_2 + m_3 = \varepsilon_3 + \varepsilon_4 - \varepsilon_3 + 0 + 0 - 0 + 0 = \varepsilon_4 = \varepsilon_1 = \varepsilon_1 + \varepsilon_2$ since $\varepsilon_1 = \varepsilon_4$ and $\varepsilon_2 = 0$. In $(\mathrm{i})_4$, $\varepsilon_3 + \varepsilon_4 - h_1 + h_3 + k_1 - k_2 + m_3 = \varepsilon_3 + \varepsilon_4 - 0 + 0 + 0 - 0 + 0 = \varepsilon_3 + \varepsilon_4 = \varepsilon_1 + \varepsilon_2$ since $\varepsilon_1 = \varepsilon_4$ and $\varepsilon_2 = \varepsilon_3$. In $(\mathrm{i})_{51}$, $\varepsilon_3 + \varepsilon_4 - h_1 + h_3 + k_1 - k_2 + m_3 = \varepsilon_3 + \varepsilon_4 - 0 + 0 + 0 - (\varepsilon_4 - \varepsilon_5) + 0 = \varepsilon_3 + \varepsilon_5 = \varepsilon_3 + \varepsilon' - \varepsilon_3 = \varepsilon' = \varepsilon_1 + \varepsilon_2$ since $\varepsilon_5 = \varepsilon' - \varepsilon_3$ and $\varepsilon' = \varepsilon_1 + \varepsilon_2$. In $(\mathrm{i})_{52}$, $\varepsilon_3 + \varepsilon_4 - h_1 + h_3 + k_1 - k_2 + m_3 = \varepsilon_3 + \varepsilon_4 - 1 + 0 + 0 - (\varepsilon_3 - 1) + 0 = \varepsilon_4 = \varepsilon' = \varepsilon_1 + \varepsilon_2$. In $(\mathrm{i})_{61}$, $\varepsilon_3 + \varepsilon_4 - h_1 + h_3 + k_1 - k_2 + m_3 = \varepsilon_3 + \varepsilon_4 - 0 + 0 + 0 - 0 + 0 = \varepsilon_3 + \varepsilon_4 = 0 + \varepsilon_4 = \varepsilon_4 = \varepsilon' = \varepsilon_1 + \varepsilon_2$. In $(\mathrm{i})_{62}$, $\varepsilon_3 + \varepsilon_4 - h_1 + h_3 + k_1 - k_2 + m_3 = \varepsilon_3 + \varepsilon_4 - 0 + 0 + 0 - 0 + 0 = \varepsilon_3 + \varepsilon_4 = 0 + \varepsilon_4 = \varepsilon_4 = \varepsilon' = \varepsilon_1 + \varepsilon_2$. In $(\mathrm{ii})_{13}$, $\varepsilon_3 + \varepsilon_4 - h_1 + h_3 + k_1 - k_2 + m_3 = \varepsilon_3 + \varepsilon_4 - (\varepsilon_4 - \varepsilon_5) + 0 + 0 - 0 + 0 = \varepsilon_3 + \varepsilon_5 = \varepsilon_3 + \varepsilon' - \varepsilon_3 = \varepsilon' = \varepsilon_1 + \varepsilon_2$. In $(\mathrm{ii})_{14}$, $\varepsilon_3 + \varepsilon_4 - h_1 + h_3 + k_1 - k_2$

$+ m_3 = \epsilon_3 + \epsilon_4 - (\epsilon_3 - \epsilon_2) + 0 + 0 - (\epsilon_4 - \epsilon_1) + 0 = \epsilon_1 + \epsilon_2$. In $(ii)_{23}$, $\epsilon_3 + \epsilon_4 - h_1 + h_3 + k_1 - k_2 + m_3 = \epsilon_3 + \epsilon_4 - 0 + 0 + 0 - 0 + 0 = \epsilon_3 + \epsilon_4 = \epsilon' + 0 = \epsilon' = \epsilon_1 + \epsilon_2$. In $(ii)_{24}$, $\epsilon_3 + \epsilon_4 - h_1 + h_3 + k_1 - k_2 + m_3 = \epsilon_3 + \epsilon_4 - 0 + 0 + 0 - \epsilon_4 + 0 = \epsilon_3 = \epsilon_2 = \epsilon_1 + \epsilon_2$ as $\epsilon_1 = 0$. In $(iii)_{111}$, $\epsilon_3 + \epsilon_4 - h_1 + h_3 + k_1 - k_2 + m_3 = \epsilon_3 + \epsilon_4 - 0 + (\epsilon_5 - \epsilon_4) + 0 - 0 + 0 = \epsilon_3 + \epsilon_5 = \epsilon_3 + \epsilon' - \epsilon_3 = \epsilon' = \epsilon_1 + \epsilon_2$. In $(iii)_{112}$, $\epsilon_3 + \epsilon_4 - h_1 + h_3 + k_1 - k_2 + m_3 = \epsilon_3 + \epsilon_4 - 0 + 0 + 0 - 0 + 0 = \epsilon_3 + \epsilon_4 = \epsilon_3 + \epsilon_5 = \epsilon_3 + \epsilon' - \epsilon_3 = \epsilon' = \epsilon_1 + \epsilon_2$. In $(iii)_{121}$, $\epsilon_3 + \epsilon_4 - h_1 + h_3 + k_1 - k_2 + m_3 = \epsilon_3 + \epsilon_4 - (\epsilon_4 - \epsilon_5) + 0 + 0 - 0 + 0 = \epsilon_3 + \epsilon_5 = \epsilon_3 + \epsilon' - \epsilon_3 = \epsilon' = \epsilon_1 + \epsilon_2$. In $(iii)_{211}$, $\epsilon_3 + \epsilon_4 - h_1 + h_3 + k_1 - k_2 + m_3 = \epsilon_3 + \epsilon_4 - 0 + (\epsilon' - \epsilon_4) + 0 - \epsilon_3 + 0 = \epsilon' = \epsilon_1 + \epsilon_2$. In $(iii)_{2211}$, $\epsilon_3 + \epsilon_4 - h_1 + h_3 + k_1 - k_2 + m_3 = \epsilon_3 + \epsilon_4 - (\epsilon_3 - \epsilon_2) + 0 + 0 - (\epsilon_4 - \epsilon_1) + 0 = \epsilon_1 + \epsilon_2$. In $(iii)_{2221}$, $\epsilon_3 + \epsilon_4 - h_1 + h_3 + k_1 - k_2 + m_3 = \epsilon_3 + \epsilon_4 - 0 + (\epsilon_2 - \epsilon_3) + 0 - (\epsilon_4 - \epsilon_1) + 0 = \epsilon_1 + \epsilon_2$. In $(iii)_{2222}$, $\epsilon_3 + \epsilon_4 - h_1 + h_3 + k_1 - k_2 + m_3 = \epsilon_3 + \epsilon_4 - 0 + 0 + 0 - (\epsilon_4 - \epsilon_1) + 0 = \epsilon_1 + \epsilon_3 = \epsilon_1 + \epsilon_2$. In $(iv)_{1311}$, $\epsilon_3 + \epsilon_4 - h_1 + h_3 + k_1 - k_2 + m_3 = \epsilon_3 + \epsilon_4 - (\epsilon_4 - \epsilon_5) + 0 + 0 - 0 + 0 = \epsilon_3 + \epsilon_5 = \epsilon_3 + \epsilon' - \epsilon_3 = \epsilon' = \epsilon_1 + \epsilon_2$. In $(iv)_{1312}$, $\epsilon_3 + \epsilon_4 - h_1 + h_3 + k_1 - k_2 + m_3 = \epsilon_3 + \epsilon_4 - 0 + 0 + 0 - 0 + 0 = \epsilon_3 + \epsilon_4$

$= \epsilon_3 + \epsilon_5 = \epsilon_3 + \epsilon' - \epsilon_3 = \epsilon' = \epsilon_1 + \epsilon_2$. In $(iv)_{1321}$, $\epsilon_3 + \epsilon_4 - h_1 + h_3 + k_1 - k_2 + m_3 = \epsilon_3 + \epsilon_4 - 0 + (\epsilon_5 - \epsilon_4) + 0 - 0 + 0 = \epsilon_3 + \epsilon_5 = \epsilon_3 + \epsilon' - \epsilon_3 = \epsilon' = \epsilon_1 + \epsilon_2$. In $(iv)_{13221}$, $\epsilon_3 + \epsilon_4 - h_1 + h_3 + k_1 - k_2 + m_3 = \epsilon_3 + \epsilon_4 - 0 + [(\epsilon_5 - 1) - \epsilon_4] + 1 - 0 + 0 = \epsilon_3 + \epsilon_5 = \epsilon_3 + \epsilon' - \epsilon_3 = \epsilon' = \epsilon_1 + \epsilon_2$. In $(iv)_{13222}$, $\epsilon_3 + \epsilon_4 - h_1 + h_3 + k_1 - k_2 + m_3 = \epsilon_3 + \epsilon_4 - 0 + [(\epsilon_5 - 1) - \epsilon_4] + 0 - 0 + 1 = \epsilon_3 + \epsilon_5 = \epsilon_3 + \epsilon' - \epsilon_3 = \epsilon' = \epsilon_1 + \epsilon_2$. In $(iv)_{1411}$, $\epsilon_3 + \epsilon_4 - h_1 + h_3 + k_1 - k_2 + m_3 = \epsilon_3 + \epsilon_4 - (\epsilon_4 - \epsilon_5) + 0 + 0 - 0 + 0 = \epsilon_3 + \epsilon_5 = \epsilon_3 + \epsilon' - \epsilon_3 = \epsilon' = \epsilon_1 + \epsilon_2$. In $(iv)_{1412}$, $\epsilon_3 + \epsilon_4 - h_1 + h_3 + k_1 - k_2 + m_3 = \epsilon_3 + \epsilon_4 - 0 + 0 + 0 - 0 + 0 = \epsilon_3 + \epsilon_4 = \epsilon_3 + \epsilon_5 = \epsilon_3 + \epsilon' - \epsilon_3 = \epsilon' = \epsilon_1 + \epsilon_2$. In $(iv)_{1421}$, $\epsilon_3 + \epsilon_4 - h_1 + h_3 + k_1 - k_2 + m_3 = \epsilon_3 + \epsilon_4 - 0 + (\epsilon_5 - \epsilon_4) + 0 - 0 + 0 = \epsilon_3 + \epsilon_5 = \epsilon_3 + \epsilon' - \epsilon_3 = \epsilon' = \epsilon_1 + \epsilon_2$. In $(iv)_{14221}$, $\epsilon_3 + \epsilon_4 - h_1 + h_3 + k_1 - k_2 + m_3 = \epsilon_3 + \epsilon_4 - 0 + [(\epsilon_5 - 1) - \epsilon_4] + 1 - 0 + 0 = \epsilon_3 + \epsilon_5 = \epsilon_3 + \epsilon' - \epsilon_3 = \epsilon' = \epsilon_1 + \epsilon_2$. In $(iv)_{14222}$, $\epsilon_3 + \epsilon_4 - h_1 + h_3 + k_1 - k_2 + m_3 = \epsilon_3 + \epsilon_4 - 0 + [(\epsilon_5 - 1) - \epsilon_4] + 0 - 0 + 1 = \epsilon_3 + \epsilon_5 = \epsilon_3 + \epsilon' - \epsilon_3 = \epsilon' = \epsilon_1 + \epsilon_2$. In $(iv)_{2311}$, $\epsilon_3 + \epsilon_4 - h_1 + h_3 + k_1 - k_2 + m_3 = \epsilon_3 + \epsilon_4 - (\epsilon_3 - \epsilon_2) + 0 + 0 - (\epsilon_4 - \epsilon_1) + 0 = \epsilon_1 + \epsilon_2$. In $(iv)_{2312}$, $\epsilon_3 + \epsilon_4 - h_1 + h_3 + k_1 - k_2 + m_3 = \epsilon_3 + \epsilon_4 - 0 + 0 + 0 - (\epsilon_4 - \epsilon_1) + 0$

$= \epsilon_1 + \epsilon_3 = \epsilon_1 + \epsilon_2$. In $(\text{iv})_{2321}$, $\epsilon_3 + \epsilon_4 - h_1 + h_3 + k_1 - k_2 + m_3 = \epsilon_3 + \epsilon_4 - 0 + (\epsilon_2 - \epsilon_3) + 0 - (\epsilon_4 - \epsilon_1) + 0 = \epsilon_1 + \epsilon_2$. In $(\text{iv})_{2411}$, $\epsilon_3 + \epsilon_4 - h_1 + h_3 + k_1 - k_2 + m_3 = \epsilon_3 + \epsilon_4 - (\epsilon_3 - \epsilon_2) + 0 + 0 - (\epsilon_4 - \epsilon_1) + 0 = \epsilon_1 + \epsilon_2$. In $(\text{iv})_{24122}$, $\epsilon_3 + \epsilon_4 - h_1 + h_3 + k_1 - k_2 + m_3 = \epsilon_3 + \epsilon_4 - 0 + 0 + 0 - (\epsilon_4 - \epsilon_1) + 0 = \epsilon_1 + \epsilon_3 = \epsilon_1 + \epsilon_2$. In $(\text{iv})_{2422}$, $\epsilon_3 + \epsilon_4 - h_1 + h_3 + k_1 - k_2 + m_3 = \epsilon_3 + \epsilon_4 - 0 + (\epsilon_2 - \epsilon_3) + 0 - (\epsilon_4 - \epsilon_1) + 0 = \epsilon_1 + \epsilon_2$. Finally in $(\text{iv})_{243}$, $\epsilon_3 + \epsilon_4 - h_1 + h_3 + k_1 - k_2 + m_3 = \epsilon_3 + \epsilon_4 - 0 + (\epsilon_2 - \epsilon_3 - 1) + 0 - 0 + 0 = \epsilon_2 + \epsilon_4 - 1 = \epsilon_2 + 1 - 1 = \epsilon_2 = \epsilon_1 + \epsilon_2$ since $\epsilon_1 = 0$. This completes the verification of (2.41).

Now from (2.38) - (2.41), obtain

$$d = (2^{\epsilon_1} D\Omega_1)(2^{\epsilon_1+\epsilon_2}\delta_2). \tag{2.42}$$

It follows from (1.1), (1.2) and (2.42) that

$$d = \Omega^2\Delta. \tag{2.43}$$

CHAPTER III

EXISTENCE OF PRIMITIVE, PROPERLY PRIMITIVE AND IMPROPERLY PRIMITIVE FORMS

Define n_1, n_2 and n_3 as the exponents of the highest powers of 2, dividing s_1, r_1 and c respectively so that

(3.1) $$s_1 = 2^{n_1} s_1', \quad s_1' \text{ odd},$$

(3.2) $$r_1 = 2^{n_2} r_1', \quad r_1' \text{ odd},$$

(3.3) $$c = 2^{n_3} c', \quad c' \text{ odd}.$$

Define P_{uv} by the condition $(u, v) = 1$, where $u, v \in \{a, b, c, r, s\}$, and u precedes v, for example, if $u = b$, then v can be c or r or s. Also note that u cannot be s and v cannot be a.

Define $P_{ab}^{(1)}$, $P_{ab}^{(2)}$, $P_{ac}^{(1)}$, $P_{ac}^{(2)}$, $P_{ar}^{(1)}$, $P_{ar}^{(2)}$, $P_{as}^{(1)}$, $P_{as}^{(2)}$, $P_{bc}^{(1)}$, $P_{bc}^{(2)}$, $P_{br}^{(1)}$, $P_{br}^{(2)}$, $P_{bs}^{(1)}$, $P_{bs}^{(2)}$, $P_{cr}^{(1)}$, $P_{cr}^{(2)}$, $P_{cs}^{(1)}$, $P_{cs}^{(2)}$, $P_{rs}^{(1)}$ and $P_{rs}^{(2)}$ by the conditions

(3.4) $$P_{ab}^{(1)}: \varepsilon_3 = 0, \ (D, \Omega_1) = 1.$$

(3.5) $$P_{ab}^{(2)}: \varepsilon_1 + \varepsilon_4 = 0, \ (D, \Omega_1) = 1.$$

(3.6) $$P_{ac}^{(1)}: \varepsilon_3 = 0, \ (a_1, c') = 1.$$

(3.7) $P_{ac}^{(2)}: n_3 = 0, \ (a_1, c') = 1.$

(3.8) $P_{ar}^{(1)}: \epsilon_3 = 0, \ (a_1, r_1') = (D, \Omega_1) = 1.$

(3.9) $P_{ar}^{(2)}: \epsilon_1 + n_2 = 0, \ (a_1, r_1') = (D, \Omega_1) = 1.$

(3.10) $P_{as}^{(1)}: \epsilon_3 = 0, \ D = 1.$

(3.11) $P_{as}^{(2)}: n_1 = 0, \ D = 1.$

(3.12) $P_{bc}^{(1)}: \epsilon_1 + \epsilon_4 = 0, \ (\Omega_1 b_2, c') = 1.$

(3.13) $P_{bc}^{(2)}: n_3 = 0, \ (\Omega_1 b_2, c') = 1.$

(3.14) $P_{br}^{(1)}: \epsilon_1 + \epsilon_4 = 0, \ \Omega_1 = (b_2, r_1') = 1.$

(3.15) $P_{br}^{(2)}: \epsilon_1 + n_2 = 0, \ \Omega_1 = (b_2, r_1') = 1.$

(3.16) $P_{bs}^{(1)}: \epsilon_1 + \epsilon_4 = 0, \ (\Omega_1, Ds_1') = (b_2, s_1') = 1.$

(3.17) $P_{bs}^{(2)}: n_1 = 0, \ (\Omega_1, Ds_1') = (b_2, s_1') = 1.$

(3.18) $P_{cr}^{(1)}: n_3 = 0, \ (c', \Omega_1 r_1') = 1.$

(3.19) $P_{cr}^{(2)}: \epsilon_1 + n_2 = 0, \ (c', \Omega_1 r_1') = 1.$

(3.20) $P_{cs}^{(1)}: n_3 = 0, \ (c', Ds_1') = 1.$

(3.21) $P_{cs}^{(2)}: n_1 = 0, \ (c', Ds_1') = 1.$

(3.22) $P_{rs}^{(1)}: \epsilon_1 + n_2 = 0, \ (\Omega_1 r_1', Ds_1') = 1.$

(3.23) $P_{rs}^{(2)}: n_1 = 0, \ (\Omega_1 r_1', Ds_1') = 1.$

Recall that ϵ_3, $\epsilon_1 + \epsilon_4$, n_3, $\epsilon_1 + n_2$ and n_1 are the exponents of the highest powers of 2, dividing a, b, c, r and s respectively.

Observe that $P_{uv}^{(1)}$ indicates that $(u, v) = 1$ and u is odd. Similarly $P_{uv}^{(2)}$ indicates that $(u, v) = 1$ and v is odd.

Lemma 3: If $(D, \Omega_1) = 1$, then $(a_2, \Omega_1) = 1$.

Proof: From (1.2), observe that D divides $\delta_1 = \Omega_1\Delta_1$. Since $(D, \Omega_1) = 1$, it follows that D divides Δ_1 and thus define Δ_2 by

(3.24) $$\Delta_1 = D\Delta_2.$$

From (1.2) and (3.24), obtain

$$D = (a_1, \delta_1) = (Da_2, \Omega_1\Delta_1) = (Da_2, D\Omega_1\Delta_2) = D(a_2, \Omega_1\Delta_2),$$

which implies that $(a_2, \Omega_1) = 1$, and the proof is complete.

Theorem 3: $P_{uv} \Leftrightarrow P_{uv}^{(1)}$ or $P_{uv}^{(2)}$, where $u, v \in \{a, b, c, r, s\}$, and u precedes v.

Proof: To prove that $P_{ab} \Leftrightarrow P_{ab}^{(1)}$ or $P_{ab}^{(2)}$, observe from (1.1) that $(a, b) = 1 \Leftrightarrow (2^{\epsilon_3}a_1, 2^{\epsilon_1+\epsilon_4}\Omega_1 b_2) = 1$, which yields

(3.25) $$\begin{cases} (a, b) = 1 \Leftrightarrow \epsilon_3 = 0,\ (a_1, \Omega_1 b_2) = 1 \text{ or} \\ \epsilon_1 + \epsilon_4 = 0,\ (a_1, \Omega_1 b_2) = 1. \end{cases}$$

Since $(a_1, b_2) = 1$ is always true by (1.2) and (1.3), it follows that

(3.26) $$(a_1, \Omega_1 b_2) = 1 \Leftrightarrow (D, \Omega_1) = 1,\ (a_2, \Omega_1) = 1.$$

By lemma 3, note that $(D, \Omega_1) = 1 \Rightarrow (a_2, \Omega_1) = 1$ and thus (3.26) reduces to

$$(a_1, \Omega_1 b_2) = 1 \Leftrightarrow (D, \Omega_1) = 1. \tag{3.27}$$

From (3.25) and (3.27), obtain $P_{ab} \Leftrightarrow P_{ab}^{(1)}$ or $P_{ab}^{(2)}$.

Next, to prove that $P_{ac} \Leftrightarrow P_{ac}^{(1)}$ or $P_{ac}^{(2)}$, observe from (1.1) and (3.3) that $(a, c) = 1 \Leftrightarrow (2^{\varepsilon_3} a_1, 2^{n_3} c') = 1$, which yields

$$\begin{cases} (a, c) = 1 \Leftrightarrow \varepsilon_3 = 0,\ (a_1, c') = 1 \text{ or } n_3 = 0, \\ (a_1, c') = 1. \end{cases} \tag{3.28}$$

Thus $P_{ac} \Leftrightarrow P_{ac}^{(1)}$ or $P_{ac}^{(2)}$ is proved.

Now to show that $P_{ar} \Leftrightarrow P_{ar}^{(1)}$ or $P_{ar}^{(2)}$, note from (1.1), (1.2), (1.13) and (3.2) that $(a, r) = 1 \Leftrightarrow (2^{\varepsilon_3} Da_2, 2^{\varepsilon_1 + n_2} \Omega_2 \Omega_3 r_1') = 1$, which yields

$$(a, r) = 1 \Leftrightarrow (2^{\varepsilon_3} Da_2, 2^{\varepsilon_1 + n_2} \Omega_1 r_1') = 1, \tag{3.29}$$

since $\Omega_1 = \Omega_2^2 \Omega_3$ by (1.2). From (3.29), obtain

$$\begin{cases} (a, r) = 1 \Leftrightarrow \varepsilon_3 = 0,\ (Da_2, \Omega_1 r_1') = 1 \text{ or} \\ \varepsilon_1 + n_2 = 0,\ (Da_2, \Omega_1 r_1') = 1. \end{cases} \tag{3.30}$$

By lemma 3 and (1.1), obtain

$$(Da_2, \Omega_1 r_1') = 1 \Leftrightarrow (a_1, r_1') = (D, \Omega_1) = 1. \tag{3.31}$$

Thus $P_{ar} \Leftrightarrow P_{ar}^{(1)}$ or $P_{ar}^{(2)}$ follows from (3.30) and (3.31).

To establish $P_{as} \Leftrightarrow P_{as}^{(1)}$ or $P_{as}^{(2)}$, note from (1.1), (1.2), (1.12) and (3.1) that $(a, s) = 1 \Leftrightarrow (2^{\varepsilon_3}Da_2, 2^{n_1}D_1D_2s_1') = 1$, which yields

$$(3.32) \qquad (a, s) = 1 \Leftrightarrow (2^{\varepsilon_3}Da_2, 2^{n_1}Ds_1') = 1,$$

since $D = D_1^2D_2$ by (1.2). From (3.32), obtain

$$(3.33) \quad \begin{cases} (a, s) = 1 \Leftrightarrow \varepsilon_3 = 0,\ D = (a_2, s_1') = 1 \text{ or} \\ n_1 = 0,\ D = (a_2, s_1') = 1. \end{cases}$$

But $(a_2, s_1') = 1$ is always true by (1.2), $(1.6)_1$ and (3.1) and thus (3.33) becomes

$$(3.34) \qquad (a, s) = 1 \Leftrightarrow \varepsilon_3 = 0,\ D = 1 \text{ or } n_1 = 0,\ D = 1.$$

Thus $P_{as} \Leftrightarrow P_{as}^{(1)}$ or $P_{as}^{(2)}$ is established.

To prove that $P_{bc} \Leftrightarrow P_{bc}^{(1)}$ or $P_{bc}^{(2)}$, observe from (1.1) and (3.3) that $(b, c) = 1 \Leftrightarrow (2^{\varepsilon_1+\varepsilon_4}\Omega_1b_2, 2^{n_3}c') = 1$, which yields

$$(3.35) \quad \begin{cases} (b, c) = 1 \Leftrightarrow \varepsilon_1 + \varepsilon_4 = 0,\ (\Omega_1b_2, c') = 1 \text{ or} \\ n_3 = 0,\ (\Omega_1b_2, c') = 1, \end{cases}$$

which proves $P_{bc} \Leftrightarrow P_{bc}^{(1)}$ or $P_{bc}^{(2)}$.

To show that $P_{br} \Leftrightarrow P_{br}^{(1)}$ or $P_{br}^{(2)}$, observe from (1.1), (1.13) and (3.2) that $(b, r) = 1 \Leftrightarrow (2^{\varepsilon_1+\varepsilon_4}\Omega_1b_2, 2^{\varepsilon_1+n_2}\Omega_2\Omega_3r_1') = 1$, which becomes

$$(3.36) \qquad (b, r) = 1 \Leftrightarrow (2^{\varepsilon_1+\varepsilon_4}\Omega_1b_2, 2^{\varepsilon_1+n_2}\Omega_1r_1') = 1,$$

since $\Omega_1 = \Omega_2^2\Omega_3$ by (1.2). From (3.36), obtain

$$(3.37)\quad \begin{cases} (b, r) = 1 \Leftrightarrow \epsilon_1 + \epsilon_4 = 0,\ \Omega_1 = (b_2, r_1') = 1 \text{ or} \\ \epsilon_1 + n_2 = 0,\ \Omega_1 = (b_2, r_1') = 1. \end{cases}$$

Thus $P_{br} \Leftrightarrow P_{br}^{(1)}$ or $P_{br}^{(2)}$ follows.

To establish $P_{bs} \Leftrightarrow P_{bs}^{(1)}$ or $P_{bs}^{(2)}$, note from (1.1), (1.12) and (3.1) that $(b, s) = 1 \Leftrightarrow (2^{\epsilon_1+\epsilon_4}\Omega_1 b_2,\ 2^{n_1}D_1D_2s_1') = 1$, which becomes

$$(3.38)\qquad (b, s) = 1 \Leftrightarrow (2^{\epsilon_1+\epsilon_4}\Omega_1 b_2,\ 2^{n_1}Ds_1') = 1,$$

since $D = D_1^2D_2$ by (1.2). From (3.38), obtain $(b, s) = 1 \Leftrightarrow \epsilon_1 + \epsilon_4 = 0,\ (\Omega_1 b_2, Ds_1') = 1$ or $n_1 = 0,\ (\Omega_1 b_2, Ds_1') = 1$, which implies that

$$(3.39)\quad \begin{cases} (b, s) = 1 \Leftrightarrow \epsilon_1 + \epsilon_4 = 0,\ (\Omega_1, Ds_1') = (b_2, s_1') = 1 \\ \text{or } n_1 = 0,\ (\Omega_1, Ds_1') = (b_2, s_1') = 1 \end{cases}$$

since $(b_2, D) = 1$ always holds by (1.2) and (1.3), and thus $P_{bs} \Leftrightarrow P_{bs}^{(1)}$ or $P_{bs}^{(2)}$ is established.

To prove that $P_{cr} \Leftrightarrow P_{cr}^{(1)}$ or $P_{cr}^{(2)}$, note from (1.13), (3.2) and (3.3) that $(c, r) = 1 \Leftrightarrow (2^{n_3}c',\ 2^{\epsilon_1+n_2}\Omega_2\Omega_3 r_1') = 1$, which yields

$$(3.40)\qquad (c, r) = 1 \Leftrightarrow (2^{n_3}c',\ 2^{\epsilon_1+n_2}\Omega_1 r_1') = 1,$$

since $\Omega_1 = \Omega_2^2\Omega_3$ by (1.2). Now (3.40) reduces to

$$(3.41) \quad \begin{cases} (c,\ r) = 1 \Leftrightarrow n_3 = 0,\ (c',\ \Omega_1 r_1') = 1 \text{ or} \\ \varepsilon_1 + n_2 = 0,\ (c',\ \Omega_1 r_1') = 1, \end{cases}$$

which proves $P_{cr} \Leftrightarrow P_{cr}^{(1)}$ or $P_{cr}^{(2)}$.

To show that $P_{cs} \Leftrightarrow P_{cs}^{(1)}$ or $P_{cs}^{(2)}$, observe from (1.12), (3.1) and (3.3) that $(c,\ s) = 1 \Leftrightarrow (2^{n_3}c',\ 2^{n_1}D_1D_2s_1') = 1$, which becomes

$$(3.42) \qquad (c,\ s) = 1 \Leftrightarrow (2^{n_3}c',\ 2^{n_1}Ds_1') = 1,$$

since $D = D_1^2D_2$ by (1.2). Now (3.42) reduces to

$$(3.43) \quad \begin{cases} (c,\ s) = 1 \Leftrightarrow n_3 = 0,\ (c',\ Ds_1') = 1 \text{ or} \\ n_1 = 0,\ (c',\ Ds_1') = 1, \end{cases}$$

which yields $P_{cs} \Leftrightarrow P_{cs}^{(1)}$ or $P_{cs}^{(2)}$.

Finally to establish $P_{rs} \Leftrightarrow P_{rs}^{(1)}$ or $P_{rs}^{(2)}$, observe from (1.12), (1.13), (3.1) and (3.2) that $(r,\ s) = 1$ $\Leftrightarrow (2^{\varepsilon_1+n_2}\Omega_2\Omega_3r_1',\ 2^{n_1}D_1D_2s_1') = 1$, which becomes

$$(3.44) \qquad (r,\ s) = 1 \Leftrightarrow (2^{\varepsilon_1+n_2}\Omega_1r_1',\ 2^{n_1}Ds_1') = 1,$$

since $\Omega_1 = \Omega_2^2\Omega_3$ and $D = D_1^2D_2$ by (1.2). From (3.44), obtain

$$(3.45) \quad \begin{cases} (r,\ s) = 1 \Leftrightarrow \varepsilon_1 + n_2 = 0,\ (\Omega_1r_1',\ Ds_1') = 1 \text{ or} \\ n_1 = 0,\ (\Omega_1r_1',\ Ds_1') = 1, \end{cases}$$

and thus $P_{rs} \Leftrightarrow P_{rs}^{(1)}$ or $P_{rs}^{(2)}$ is established and the proof of theorem 3 is complete.

Corollary 3: A form $f = ax^2 + by^2 + cz^2 + 2ryz + 2sxz$ is primitive iff at least one of the conditions $P_{uv}^{(i)}$ is satisfied, where $i = 1,\ 2;\ u,\ v \in \{a,\ b,\ c,\ r,\ s\}$, and u precedes v.

Proof: By the definition of a primitive form, it follows that a form $f = ax^2 + by^2 + cz^2 + 2ryz + 2sxz$ is primitive iff at least two of a, b, c, r and s are relatively prime; that is, iff P_{uv} is satisfied for at least one u and one v from the set {a, b, c, r, s}, where u precedes v. Now it follows from theorem 3 that a form f is primitive iff at least one of the conditions $P_{uv}^{(i)}$ is satisfied, where $i = 1, 2$; $u, v \in \{a, b, c, r, s\}$, and u precedes v.

Remark: Observe from (3.4), (3.8) and (3.10) that $P_{as}^{(1)}$ or $P_{ar}^{(1)} \Rightarrow P_{ab}^{(1)}$, that is, if there exists a primitive form with $(a, s) = 1$, a odd or $(a, r) = 1$, a odd, then $(a, b) = 1$ in that form. Similarly from (3.5), (3.14) and (3.16), observe that $P_{bs}^{(1)}$ or $P_{br}^{(1)} \Rightarrow P_{ab}^{(2)}$, that is, if there exists a primitive form with $(b, s) = 1$, b odd or $(b, r) = 1$, b odd, then $(a, b) = 1$ in that form.

Determination of primitive, properly primitive and improperly primitive forms for subcases in the summaries of theorem 1:

To determine which of the existing forms of theorem 1 are primitive, and also properly or improperly primitive, examine the subcases in the summaries of theorem 1 as follows:

In all subcases except $(iv)_{13222}$ and $(iv)_{14222}$, if $n_3 = 0$, then each of $P_{ac}^{(2)}$, $P_{bc}^{(2)}$, $P_{cr}^{(1)}$ and $P_{cs}^{(1)}$ is satisfied according as (a_1, c'), $(\Omega_1 b_2, c')$, $(c', \Omega_1 r_1')$ and (c', Ds_1') is equal to one.

Case (i) $\varepsilon_3 \le \varepsilon' \le \varepsilon_4$:

In all subcases of (i), if $n_1 = 0$, then each of $P^{(2)}_{as}$, $P^{(2)}_{bs}$, $P^{(2)}_{cs}$ and $P^{(2)}_{rs}$ is satisfied according as $D = 1$, $(\Omega_1, Ds_1') = (b_2, s_1') = 1$, $(c', Ds_1') = 1$ and $(\Omega_1 r_1', Ds_1') = 1$.

Subcase $(i)_1$

$$\left\{\begin{array}{l}
\underline{\varepsilon_2 < \varepsilon_3,\ \varepsilon_1 < \varepsilon_4 = \varepsilon'},\ h_1 = \varepsilon_3 - \varepsilon_2,\ k_2 = \varepsilon_4 \\
-\ \varepsilon_1,\ A = 2^{\varepsilon_1}A_2,\ s_1A_2r_1 \text{ odd},\ c \equiv 0 \text{ or } 1 \pmod 2 \\
\text{according as } r_1 \text{ satisfies } \Omega_3 r_1^2 + A_2 \equiv 0 \\
\text{or } 2^{\varepsilon_4-\varepsilon_1} \pmod{2^{\varepsilon_4-\varepsilon_1+1}}.
\end{array}\right.$$

If $\varepsilon_3 = 0$, then $\varepsilon_2 < \varepsilon_3 \Rightarrow \varepsilon_2 < 0$, which is impossible, and thus $P^{(1)}_{ab}$, $P^{(1)}_{ac}$, $P^{(1)}_{ar}$ and $P^{(1)}_{as}$ are not satisfied. $\varepsilon_1 + \varepsilon_4 = 0$ is impossible since $\varepsilon_1 < \varepsilon_4$, and thus $P^{(2)}_{ab}$, $P^{(1)}_{bc}$, $P^{(1)}_{br}$ and $P^{(1)}_{bs}$ are not satisfied. If $\varepsilon_1 + n_2 = 0$, then $\varepsilon_1 = n_2 = 0$. But $\varepsilon_1 = 0$ and $\varepsilon_3 \le \varepsilon' = \varepsilon_1 + \varepsilon_2$ $\Rightarrow \varepsilon_3 \le \varepsilon_2$, which is impossible since $\varepsilon_2 < \varepsilon_3$, and thus $P^{(2)}_{ar}$, $P^{(2)}_{br}$, $P^{(2)}_{cr}$ and $P^{(1)}_{rs}$ are not satisfied. Further, the existing primitive form is properly primitive iff c is odd.

Subcase $(i)_2$

$$\left\{\begin{array}{l}
\underline{\varepsilon_2 = \varepsilon_3,\ \varepsilon_1 < \varepsilon_4},\ h_2 = \varepsilon_4 - \varepsilon',\ k_2 = \varepsilon_4 - \varepsilon_1, \\
A = 2^{\varepsilon_5}A_1,\ A_1r_1 \text{ odd if } \varepsilon_4 > \varepsilon';\ \text{if } \varepsilon_4 = \varepsilon', \\
\text{then } A_1r_1 \equiv s_1 + 1 \equiv 1 \pmod 2 \text{ or} \\
(A_1/4)(r_1/2)s_1 \equiv 1 \pmod 2;\ c \equiv 0 \text{ or } 1 \pmod 2 \\
\text{according as } r_1 \text{ satisfies } \Omega_3 r_1^2 + A_1 \equiv 0 \\
\text{or } 2^{\varepsilon_4-\varepsilon_1} \pmod{2^{\varepsilon_4-\varepsilon_1+1}}.
\end{array}\right.$$

If $\varepsilon_3 = 0$, then each of $P^{(1)}_{ab}$, $P^{(1)}_{ac}$, $P^{(1)}_{ar}$ and $P^{(1)}_{as}$ is satisfied according as $(D, \Omega_1) = 1$, $(a_1, c') = 1$, $(a_1, r_1') = (D, \Omega_1) = 1$ and $D = 1$. $\varepsilon_1 + \varepsilon_4 = 0$ is impossible since $\varepsilon_1 < \varepsilon_4$, and thus $P^{(2)}_{ab}$, $P^{(1)}_{bc}$, $P^{(1)}_{br}$ and $P^{(1)}_{bs}$ are not satisfied. If $\varepsilon_1 + n_2 = 0$, then each of $P^{(2)}_{ar}$, $P^{(2)}_{br}$, $P^{(2)}_{cr}$ and $P^{(1)}_{rs}$ is satisfied according as $(a_1, r_1') = (D, \Omega_1) = 1$, $\Omega_1 = (b_2, r_1') = 1$, $(c', \Omega_1 r_1') = 1$ and $(\Omega_1 r_1', Ds_1') = 1$. Further, the existing primitive form is properly primitive iff a or c is odd.

Subcase (i)$_3$
$$\left\{\begin{array}{l} 0 = \varepsilon_2 < \varepsilon_3,\ \varepsilon_1 = \varepsilon_4,\ h_1 = \varepsilon_3,\ A = 2^{\varepsilon_1}A_2, \\ s_1 \text{ odd, } A_2 \equiv 0 \text{ or } 1 \pmod 2 \text{ according as} \\ s_1 \text{ is chosen to satisfy } b_2D_2s_1^2 + \delta_2 \equiv 0 \\ \text{or } 2^{\varepsilon_3} \pmod{2^{\varepsilon_3+1}},\ c \equiv A_2 + r_1 \pmod 2. \end{array}\right.$$

$\varepsilon_3 = 0$ is impossible in this subcase, and thus $P^{(1)}_{ab}$, $P^{(1)}_{ac}$, $P^{(1)}_{ar}$ and $P^{(1)}_{as}$ are not satisfied. $\varepsilon_1 + \varepsilon_4 = 0$ and $\varepsilon_3 \le \varepsilon' = \varepsilon_1 + \varepsilon_2 \le \varepsilon_4 \Rightarrow \varepsilon_3 \le \varepsilon_2 \le 0 \Rightarrow \varepsilon_3 = 0$, which is impossible, and thus $P^{(2)}_{ab}$, $P^{(1)}_{bc}$, $P^{(1)}_{br}$ and $P^{(1)}_{bs}$ are not satisfied. If $\varepsilon_1 + n_2 = 0$, then $\varepsilon_1 = n_2 = 0$. Now $\varepsilon_1 = 0$ and $\varepsilon_1 = \varepsilon_4 \Rightarrow \varepsilon_1 = \varepsilon_4 = 0$, which is impossible by the preceding argument, and thus $P^{(2)}_{ar}$, $P^{(2)}_{br}$, $P^{(2)}_{cr}$ and $P^{(1)}_{rs}$ are not satisfied. Moreover, the existing primitive form is properly primitive iff c is odd.

Subcase (i)$_4$
$$\left\{\begin{array}{l} 0 = \varepsilon_2 = \varepsilon_3,\ \varepsilon_1 = \varepsilon_4,\ A = 2^{\varepsilon_1}A_1,\ A_1 \equiv s_1 + 1 \\ \pmod 2,\ c \equiv r_1 + s_1 + 1 \pmod 2. \end{array}\right.$$

Since $\epsilon_3 = 0$, each of $P_{ab}^{(1)}$, $P_{ac}^{(1)}$, $P_{ar}^{(1)}$ and $P_{as}^{(1)}$ is satisfied according as $(D, \Omega_1) = 1$, $(a_1, c') = 1$, $(a_1, r_1') = (D, \Omega_1) = 1$ and $D = 1$. If $\epsilon_1 + \epsilon_4 = 0$, then each of $P_{ab}^{(2)}$, $P_{bc}^{(1)}$, $P_{br}^{(1)}$ and $P_{bs}^{(1)}$ is satisfied according as $(D, \Omega_1) = 1$, $(\Omega_1 b_2, c') = 1$, $\Omega_1 = (b_2, r_1') = 1$ and $(\Omega_1, Ds_1') = (b_2, s_1') = 1$. If $\epsilon_1 + n_2 = 0$, then each of $P_{ar}^{(2)}$, $P_{br}^{(2)}$, $P_{cr}^{(2)}$ and $P_{rs}^{(1)}$ is satisfied according as $(a_1, r_1') = (D, \Omega_1) = 1$, $\Omega_1 = (b_2, r_1') = 1$, $(c', \Omega_1 r_1') = 1$ and $(\Omega_1 r_1', Ds_1') = 1$. Moreover, the existing primitive form is properly primitive since a is odd.

Subcase $(i)_{51}$
$$\left\{\begin{array}{l} \underline{\epsilon_3 < \epsilon_2,\ \epsilon_5 < \epsilon_4,\ \epsilon_3 \equiv \epsilon_2 \pmod 2},\ h_2 = \epsilon_4 - \epsilon' \\ k_2 = \epsilon_4 - \epsilon_5,\ A = 2^{\epsilon_5} A_1,\ r_1 = 2^{(\epsilon_2 - \epsilon_3)/2} r_2, \\ A_1 r_2 \text{ odd if } \epsilon_4 > \epsilon';\ A_1 r_2 \equiv s_1 + 1 \equiv 1 \pmod 2 \\ \text{or } (A_1/4)(r_2/2) s_1 \equiv 1 \pmod 2 \text{ if } \epsilon_4 = \epsilon'; \\ c \equiv 0 \text{ or } 1 \pmod 2 \text{ according as } r_2 \text{ satisfies} \\ \Omega_3 r_2^2 + A_1 \equiv 0 \text{ or } 2^{\epsilon_4 - \epsilon_5} \pmod{2^{\epsilon_4 - \epsilon_5 + 1}}. \end{array}\right.$$

If $\epsilon_3 = 0$, then each of $P_{ab}^{(1)}$, $P_{ac}^{(1)}$, $P_{ar}^{(1)}$ and $P_{as}^{(1)}$ is satisfied according as $(D, \Omega_1) = 1$, $(a_1, c') = 1$, $(D, \Omega_1) = (a_1, r_1') = 1$ and $D = 1$. If $\epsilon_1 + \epsilon_4 = 0$, then $\epsilon_5 = \epsilon' - \epsilon_3 = \epsilon_1 + \epsilon_2 - \epsilon_3 < \epsilon_4 \Rightarrow \epsilon_2 - \epsilon_3 < 0 \Rightarrow \epsilon_2 < \epsilon_3$, which is impossible since $\epsilon_3 < \epsilon_2$, and thus $P_{ab}^{(2)}$, $P_{bc}^{(1)}$, $P_{br}^{(1)}$ and $P_{bs}^{(1)}$ are not satisfied. If $\epsilon_1 + n_2 = 0$, then $\epsilon_1 = n_2 = 0$. But

$n_2 = 0 \Rightarrow r_1$ is odd, which is impossible since $r_1 = 2^{(\epsilon_2-\epsilon_3)/2} r_2$, $\epsilon_3 < \epsilon_2$ and $\epsilon_3 \equiv \epsilon_2 \pmod 2 \Rightarrow r_1$ is even, and thus $P^{(2)}_{ar}$, $P^{(2)}_{br}$, $P^{(2)}_{cr}$ and $P^{(1)}_{rs}$ are not satisfied. Further, the existing primitive form is properly primitive iff a or c is odd.

Subcase $(i)_{52}$

$$\begin{cases} 0 < \epsilon_3 < \epsilon_2,\ \epsilon_4 = \epsilon',\ \epsilon_3 \equiv \epsilon_2 + 1 \pmod 2, \\ h_1 = 1,\ k_2 = \epsilon_3 - 1,\ A = 2^{\epsilon_5+1} A_2, \\ r_1 = 2^{(\epsilon_2-\epsilon_3+1)/2} r_2,\ s_1 \text{ odd},\ c \equiv 0 \text{ or } 1 \pmod 2 \\ \text{according as } r_2 \text{ satisfies } \Omega_3 r_2^2 + A_2 \equiv 0 \\ \text{or } 2^{\epsilon_3-1} \pmod{2^{\epsilon_3}}. \end{cases}$$

Since $\epsilon_3 = 0$ is impossible, $P^{(1)}_{ab}$, $P^{(1)}_{ac}$, $P^{(1)}_{ar}$ and $P^{(1)}_{as}$ are not satisfied. If $\epsilon_1 + \epsilon_4 = 0$, then $\epsilon_4 = \epsilon' = \epsilon_1 + \epsilon_2 \Rightarrow \epsilon_2 = 0$, which is impossible since $\epsilon_2 > 0$, and thus $P^{(2)}_{ab}$, $P^{(1)}_{bc}$, $P^{(1)}_{br}$ and $P^{(1)}_{bs}$ are not satisfied. If $\epsilon_1 + n_2 = 0$, then $\epsilon_1 = n_2 = 0$. Now $n_2 = 0 \Rightarrow r_1$ is odd, which is impossible since $r_1 = 2^{(\epsilon_2-\epsilon_3+1)/2} r_2$, $0 < \epsilon_3 < \epsilon_2$ and $\epsilon_3 \equiv \epsilon_2 + 1 \pmod 2 \Rightarrow r_1$ is even, and thus $P^{(2)}_{ar}$, $P^{(2)}_{br}$, $P^{(2)}_{cr}$ and $P^{(1)}_{rs}$ are not satisfied. Moreover, the existing primitive form is properly primitive iff c is odd.

Subcase $(i)_{61}$

$$\begin{cases} 0 = \epsilon_3 < \epsilon_2,\ \epsilon' = \epsilon_4,\ \epsilon_2 \equiv 0 \pmod 2, \\ A = 2^{\epsilon_5} A_1,\ r_1 = 2^{\epsilon_2/2} r_2,\ A_1 \equiv s_1 + 1 \pmod 2, \\ c \equiv s_1 + r_2 + 1 \pmod 2. \end{cases}$$

Since $\varepsilon_3 = 0$, each of $P_{ab}^{(1)}$, $P_{ac}^{(1)}$, $P_{ar}^{(1)}$ and $P_{as}^{(1)}$ is satisfied according as $(D, \Omega_1) = 1$, $(a_1, c') = 1$, $(a_1, r_1') = (D, \Omega_1) = 1$ and $D = 1$. If $\varepsilon_1 + \varepsilon_4 = 0$, then $\varepsilon' = \varepsilon_1 + \varepsilon_2 = \varepsilon_4 \Rightarrow \varepsilon_2 = 0$, which is impossible since $\varepsilon_2 > 0$, and thus $P_{ab}^{(2)}$, $P_{bc}^{(1)}$, $P_{br}^{(1)}$ and $P_{bs}^{(1)}$ are not satisfied. If $\varepsilon_1 + n_2 = 0$, then $\varepsilon_1 = n_2 = 0$. Now $n_2 = 0 \Rightarrow r_1$ is odd, which is impossible since $r_1 = 2^{\varepsilon_2/2} r_2$, $\varepsilon_2 > 0$ and $\varepsilon_2 \equiv 0 \pmod{2} \Rightarrow r_1$ is even, and thus $P_{ar}^{(2)}$, $P_{br}^{(2)}$, $P_{cr}^{(2)}$ and $P_{rs}^{(1)}$ are not satisfied. Moreover, the existing primitive form is properly primitive.

Subcase $(i)_{62}$ $\left\{ \begin{array}{l} 0 = \varepsilon_3 < \varepsilon_2,\ \varepsilon' = \varepsilon_4,\ \varepsilon_2 \equiv 1 \pmod{2},\ k_3 = 1, \\ A = 2^{\varepsilon_5} A_1,\ r_1 = 2^{(\varepsilon_2+1)/2} r_2,\ c \equiv A_1 \equiv s_1 + 1 \\ \pmod{2}. \end{array} \right.$

Since $\varepsilon_3 = 0$, each of $P_{ab}^{(1)}$, $P_{ac}^{(1)}$, $P_{ar}^{(1)}$ and $P_{as}^{(1)}$ is satisfied according as $(D, \Omega_1) = 1$, $(a_1, c') = 1$, $(a_1, r_1') = (D, \Omega_1) = 1$ and $D = 1$. If $\varepsilon_1 + \varepsilon_4 = 0$, then $\varepsilon' = \varepsilon_1 + \varepsilon_2 = \varepsilon_4 \Rightarrow \varepsilon_2 = 0$, which is impossible since $\varepsilon_2 > 0$, and thus $P_{ab}^{(2)}$, $P_{bc}^{(1)}$, $P_{br}^{(1)}$ and $P_{bs}^{(1)}$ are not satisfied. If $\varepsilon_1 + n_2 = 0$, then $\varepsilon_1 = n_2 = 0$. Now $n_2 = 0 \Rightarrow r_1$ is odd, which is impossible since $r_1 = 2^{(\varepsilon_2+1)/2} r_2$ and $\varepsilon_2 \equiv 1 \pmod{2} \Rightarrow r_1$ is even, and thus $P_{ar}^{(2)}$, $P_{br}^{(2)}$, $P_{cr}^{(2)}$ and $P_{rs}^{(1)}$ are not satisfied. Further, the existing primitive form is properly primitive.

Case (ii) $\epsilon_4 \le \epsilon' \le \epsilon_3$, $\epsilon_4 \ne \epsilon_3$, $s_1 = 2^{[(\epsilon'-\epsilon_4+1)/2]} s_2$:

If $\epsilon_3 = 0$, then $\epsilon_4 \le \epsilon' \le \epsilon_3 \Rightarrow \epsilon_4 \le \epsilon' \le 0 \Rightarrow \epsilon_4 = 0$, which is impossible since $\epsilon_4 \ne \epsilon_3$, and thus $P_{ab}^{(1)}$, $P_{ac}^{(1)}$, $P_{ar}^{(1)}$ and $P_{as}^{(1)}$ are not satisfied in any subcase of (ii). In all subcases of (ii), if $\epsilon_1 + n_2 = 0$, then each of $P_{ar}^{(2)}$, $P_{br}^{(2)}$, $P_{cr}^{(2)}$ and $P_{rs}^{(1)}$ is satisfied according as $(a_1, r_1') = (D, \Omega_1) = 1$, $\Omega_1 = (b_2, r_1') = 1$, $(c', \Omega_1 r_1') = 1$ and $(\Omega_1 r_1', Ds_1') = 1$.

Subcase (ii)$_{13}$

$$\left\{\begin{array}{l} \epsilon_4 < \epsilon_1,\ \epsilon_4 \equiv \epsilon' \pmod{2},\ h_1 = \epsilon_4 - \epsilon_5, \\ k_3 = \epsilon_1 - \epsilon_4,\ A = 2^{\epsilon_4} A_1,\ s_2 \text{ odd if } \epsilon_5 < \epsilon_4, \\ A_1 \equiv 0 \text{ or } 1 \pmod{2} \text{ according as } s_2 \text{ is} \\ \text{chosen to satisfy } b_2 D_2 s_2^2 + \delta_2 \equiv 0 \text{ or} \\ 2^{\epsilon_4-\epsilon_5} \pmod{2^{\epsilon_4-\epsilon_5+1}},\ c \equiv A_1 + 2^{\epsilon_1-\epsilon_4} r_1 \\ \pmod{2}. \end{array}\right.$$

If $\epsilon_1 + \epsilon_4 = 0$, then each of $P_{ab}^{(2)}$, $P_{bc}^{(1)}$, $P_{br}^{(1)}$ and $P_{bs}^{(1)}$ is satisfied according as $(D, \Omega_1) = 1$, $(\Omega_1 b_2, c') = 1$, $\Omega_1 = (b_2, r_1') = 1$ and $(\Omega_1, Ds_1') = (b_2, s_1') = 1$. If $n_1 = 0$, then s_1 is odd. Now $s_1 = 2^{[(\epsilon'-\epsilon_4+1)/2]} s_2$, $\epsilon_4 \equiv \epsilon' \pmod{2}$ and s_1 odd $\Rightarrow \epsilon_4 = \epsilon'$ and s_2 odd, and thus each of $P_{as}^{(2)}$, $P_{bs}^{(2)}$, $P_{cs}^{(2)}$ and $P_{rs}^{(2)}$ is satisfied according as $D = 1$, $(\Omega_1, Ds_1') = (b_2, s_1') = 1$, $(c', Ds_1') = 1$ and $(\Omega_1 r_1', Ds_1') = 1$. Further, the existing primitive form is properly primitive iff b or c is odd.

Subcase (ii)$_{14}$

$$\left\{\begin{array}{l} \epsilon_4 > \epsilon_1,\ \epsilon_4 \equiv \epsilon' \pmod 2,\ h_1 = \epsilon_3 - \epsilon_2, \\ k_2 = \epsilon_4 - \epsilon_1,\ A = 2^{\epsilon_1}A_1,\ s_2A_1r_1 \text{ odd if} \\ \epsilon_2 < \epsilon_3;\ A_1r_1 \equiv s_2 + 1 \equiv 1 \pmod 2 \text{ or} \\ (A_1/4)(r_1/2)s_2 \equiv 1 \pmod 2 \text{ if } \epsilon_2 = \epsilon_3; \\ c \equiv 0 \text{ or } 1 \pmod 2 \text{ according as } r_1 \text{ satisfies} \\ \Omega_3 r_1^2 + A_1 \equiv 0 \text{ or } 2^{\epsilon_4-\epsilon_1} \pmod{2^{\epsilon_4-\epsilon_1+1}}. \end{array}\right.$$

$\epsilon_1 + \epsilon_4 = 0$ is impossible since $\epsilon_4 > \epsilon_1$, and thus $P^{(2)}_{ab}$, $P^{(1)}_{bc}$, $P^{(1)}_{br}$ and $P^{(1)}_{bs}$ are not satisfied. If $n_1 = 0$, then s_1 is odd. Now $s_1 = 2^{[(\epsilon'-\epsilon_4+1)/2]} s_2$, $\epsilon_4 \equiv \epsilon'$ (mod 2) and s_1 odd $\Rightarrow$ $\epsilon_4 = \epsilon'$ and s_2 odd, and thus each of $P^{(2)}_{as}$, $P^{(2)}_{bs}$, $P^{(2)}_{cs}$ and $P^{(2)}_{rs}$ is satisfied according as $D = 1$, $(\Omega_1, Ds_1') = (b_2, s_1') = 1$, $(c', Ds_1') = 1$ and $(\Omega_1 r_1', Ds_1') = 1$. Moreover, the existing primitive form is properly primitive iff c is odd.

Subcase (ii)$_{23}$

$$\left\{\begin{array}{l} 0 = \epsilon_4 \equiv \epsilon' + 1 \pmod 2,\ \epsilon_3 = \epsilon',\ h_2 = 1, \\ k_3 = \epsilon_1,\ A \text{ odd},\ c \equiv r_1 + 1 \text{ or } 1 \pmod 2 \\ \text{according as } \epsilon_1 = 0 \text{ or } \epsilon_1 > 0. \end{array}\right.$$

If $\epsilon_1 + \epsilon_4 = 0$, then each of $P^{(2)}_{ab}$, $P^{(1)}_{bc}$, $P^{(1)}_{br}$ and $P^{(1)}_{bs}$ is satisfied according as $(D, \Omega_1) = 1$, $(\Omega_1 b_2, c') = 1$, $\Omega_1 = (b_2, r_1') = 1$ and $(\Omega_1, Ds_1') = (b_2, s_1') = 1$. If $n_1 = 0$, then s_1 is odd. But $s_1 = 2^{[(\epsilon'-\epsilon_4+1)/2]} s_2$, $0 = \epsilon_4 \equiv \epsilon' + 1$ (mod 2) and s_1 odd $\Rightarrow$ s_2 odd and $\epsilon' + 1 = 0$, which is impossible since ε' is non-negative, and thus $P_{as}^{(2)}$, $P_{bs}^{(2)}$, $P_{cs}^{(2)}$ and $P_{rs}^{(2)}$ are not satisfied. Furthermore, the existing primitive form is properly primitive iff b or c is odd.

Subcase $(\text{ii})_{24}$
$$\begin{cases} \varepsilon_1 = 0 < \varepsilon_4 \equiv \varepsilon_2 + 1 \pmod 2,\ \varepsilon_3 = \varepsilon_2, \\ h_2 = 1,\ k_2 = \varepsilon_4,\ Ar_1 \text{ odd},\ c \equiv 0 \text{ or } 1 \pmod 2 \\ \text{according as } r_1 \text{ satisfies } \Omega_3 r_1^2 + A \equiv 0 \text{ or} \\ 2^{\varepsilon_4} \pmod{2^{\varepsilon_4+1}}. \end{cases}$$

$\varepsilon_1 + \varepsilon_4 = 0$ is impossible since $\varepsilon_4 > 0$, and thus $P_{ab}^{(2)}$, $P_{bc}^{(1)}$, $P_{br}^{(1)}$ and $P_{bs}^{(1)}$ are not satisfied. If $n_1 = 0$, then s_1 is odd. But $s_1 = 2^{[(\varepsilon'-\varepsilon_4+1)/2]} s_2$, $\varepsilon_1 = 0 < \varepsilon_4 \equiv \varepsilon_2 + 1 \pmod 2$ and s_1 odd $\Rightarrow$ s_2 odd and $\varepsilon_4 = \varepsilon_2 + 1$, that is, $\varepsilon_4 > \varepsilon_2$, which is impossible since $\varepsilon_4 \le \varepsilon'$ and $\varepsilon_1 = 0 \Rightarrow \varepsilon_4 \le \varepsilon_2$, and thus $P_{as}^{(2)}$, $P_{bs}^{(2)}$, $P_{cs}^{(2)}$ and $P_{rs}^{(2)}$ are not satisfied. Moreover, the existing primitive form is properly primitive iff c is odd.

Case (iii) $\varepsilon_3 \le \varepsilon_4 < \varepsilon'$:

Subcase $(\text{iii})_{111}$
$$\begin{cases} \varepsilon_4 \le \varepsilon_1,\ \varepsilon_4 \le \varepsilon_5,\ \varepsilon_3 \equiv 0 \pmod 2, \\ h_3 = \varepsilon_5 - \varepsilon_4,\ k_3 = \varepsilon_1 - \varepsilon_4,\ A = 2^{\varepsilon_4} A_2, \\ s_1 = 2^{\varepsilon_3/2} s_2,\ A_2 \equiv s_2 + 2^{\varepsilon_5-\varepsilon_4} \pmod 2, \\ c \equiv A_2 + 2^{\varepsilon_1-\varepsilon_4} r_1 \pmod 2. \end{cases}$$

If $\varepsilon_3 = 0$, then each of $P_{ab}^{(1)}$, $P_{ac}^{(1)}$, $P_{ar}^{(1)}$ and $P_{as}^{(1)}$

is satisfied according as $(D, \Omega_1) = 1$, $(a_1, c') = 1$, $(a_1, r_1') = (D, \Omega_1) = 1$ and $D = 1$. If $\epsilon_1 + \epsilon_4 = 0$, then each of $P^{(2)}_{ab}$, $P^{(1)}_{bc}$, $P^{(1)}_{br}$ and $P^{(1)}_{bs}$ is satisfied according as $(D, \Omega_1) = 1$, $(\Omega_1 b_2, c') = 1$, $\Omega_1 = (b_2, r_1') = 1$ and $(\Omega_1, Ds_1') = (b_2, s_1') = 1$. If $\epsilon_1 + n_2 = 0$, then each of $P^{(2)}_{ar}$, $P^{(2)}_{br}$, $P^{(2)}_{cr}$ and $P^{(1)}_{rs}$ is satisfied according as $(a_1, r_1') = (D, \Omega_1) = 1$, $\Omega_1 = (b_2, r_1') = 1$, $(c', \Omega_1 r_1') = 1$ and $(\Omega_1 r_1', Ds_1') = 1$. If $n_1 = 0$, then s_1 is odd. Now $s_1 = 2^{\epsilon_3/2} s_2$ and s_1 odd $\Rightarrow \epsilon_3 = 0$ and s_2 odd, and thus each of $P^{(2)}_{as}$, $P^{(2)}_{bs}$, $P^{(2)}_{cs}$ and $P^{(2)}_{rs}$ is satisfied according as $D = 1$, $(\Omega_1, Ds_1') = (b_2, s_1') = 1$, $(c', Ds_1') = 1$ and $(\Omega_1 r_1', Ds_1') = 1$. Further, the existing primitive form is properly primitive iff at least one of a, b and c is odd.

Subcase $(\text{iii})_{112}$

$$\begin{cases} \underline{\epsilon_4 \le \epsilon_1,\ \epsilon_4 = \epsilon_5,\ \epsilon_3 \equiv 1 \pmod{2},} \\ h_2 = 1,\ k_3 = \epsilon_1 - \epsilon_4,\ A = 2^{\epsilon_4} A_2,\ A_2 \text{ odd}, \\ s_1 = 2^{(\epsilon_3+1)/2} s_2,\ c \equiv 1 + 2^{\epsilon_1 - \epsilon_4} r_1 \pmod{2}. \end{cases}$$

$\epsilon_3 = 0$ is impossible since $\epsilon_3 \equiv 1 \pmod{2}$, and thus $P^{(1)}_{ab}$, $P^{(1)}_{ac}$, $P^{(1)}_{ar}$ and $P^{(1)}_{as}$ are not satisfied. If $\epsilon_1 + \epsilon_4 = 0$, then $\epsilon_1 = \epsilon_4 = 0$. But $\epsilon_4 = 0$ and $\epsilon_3 \le \epsilon_4 \Rightarrow \epsilon_3 = 0$, which is impossible since $\epsilon_3 \equiv 1 \pmod{2}$, and thus $P^{(2)}_{ab}$, $P^{(1)}_{bc}$, $P^{(1)}_{br}$ and $P^{(1)}_{bs}$ are not satisfied. If $\epsilon_1 + n_2 = 0$, then $\epsilon_1 = n_2 = 0$.

But $\varepsilon_1 = 0$ and $\varepsilon_4 \le \varepsilon_1 \Rightarrow \varepsilon_4 = 0$. Now $\varepsilon_4 = 0$ and $\varepsilon_3 \le \varepsilon_4 \Rightarrow \varepsilon_3 \le 0 \Rightarrow \varepsilon_3 = 0$, which is impossible since $\varepsilon_3 \equiv 1 \pmod 2$, and thus $P^{(2)}_{ar}$, $P^{(2)}_{br}$, $P^{(2)}_{cr}$ and $P^{(1)}_{rs}$ are not satisfied. If $n_1 = 0$, then s_1 is odd. But $s_1 = 2^{(\varepsilon_3+1)/2} s_2$, $\varepsilon_3 \equiv 1 \pmod 2$ and s_1 odd $\Rightarrow \varepsilon_3 + 1 = 0$, which is impossible since ε_3 is non-negative, and thus $P^{(2)}_{as}$, $P^{(2)}_{bs}$, $P^{(2)}_{cs}$ and $P^{(2)}_{rs}$ are not satisfied. Further, the existing primitive form is properly primitive since a primitive form exists in this subcase iff c is odd.

Subcase $(\text{iii})_{121}$

$$\left\{\begin{array}{l} \varepsilon_4 \le \varepsilon_1,\ \varepsilon_4 > \varepsilon_5,\ \varepsilon_4 \equiv \varepsilon' \pmod 2, \\ h_1 = \varepsilon_4 - \varepsilon_5,\ k_3 = \varepsilon_1 - \varepsilon_4,\ A = 2^{\varepsilon_4} A_2, \\ s_1 = 2^{(\varepsilon'-\varepsilon_4)/2} s_2,\ s_2 \text{ odd},\ A_2 \equiv 0 \\ \text{or } 1 \pmod 2 \text{ according as } s_2 \text{ satisfies} \\ b_2 D_2 s_2^2 + \delta_2 \equiv 0 \text{ or } 2^{\varepsilon_4-\varepsilon_5} \pmod{2^{\varepsilon_4-\varepsilon_5+1}}, \\ c \equiv A_2 + 2^{\varepsilon_1-\varepsilon_4} r_1 \pmod 2. \end{array}\right.$$

If $\varepsilon_3 = 0$, then $\varepsilon_4 > \varepsilon_5 = \varepsilon' - \varepsilon_3 \Rightarrow \varepsilon_4 > \varepsilon'$, which is impossible since $\varepsilon_4 < \varepsilon'$, and thus $P^{(1)}_{ab}$, $P^{(1)}_{ac}$, $P^{(1)}_{ar}$ and $P^{(1)}_{as}$ are not satisfied. If $\varepsilon_1 + \varepsilon_4 = 0$, then $\varepsilon_1 = \varepsilon_4 = 0$. But $\varepsilon_4 = 0$ and $\varepsilon_3 \le \varepsilon_4 \Rightarrow \varepsilon_3 = 0$, which is impossible by the preceding argument, and thus $P^{(2)}_{ab}$, $P^{(1)}_{bc}$, $P^{(1)}_{br}$ and $P^{(1)}_{bs}$ are not satisfied. If $\varepsilon_1 + n_2 = 0$, then $\varepsilon_1 = n_2 = 0$. But $\varepsilon_1 = 0$ and $\varepsilon_4 \le \varepsilon_1 \Rightarrow \varepsilon_4 = 0$, which is impossible by the preceding argument, and thus $P^{(2)}_{ar}$, $P^{(2)}_{br}$, $P^{(2)}_{cr}$ and $P^{(1)}_{rs}$ are not satisfied. If $n_1 = 0$, then s_1 is odd. But $s_1 = 2^{(\varepsilon' - \varepsilon_4)/2} s_2$, s_2 odd and s_1 odd $\Rightarrow \varepsilon_4 = \varepsilon'$, which is impossible since $\varepsilon_4 < \varepsilon'$, and thus $P^{(2)}_{as}$, $P^{(2)}_{bs}$, $P^{(2)}_{cs}$ and $P^{(2)}_{rs}$ are not satisfied. Moreover, the existing primitive form is properly primitive.

Subcase $(\text{iii})_{211}$

$$\begin{cases} \varepsilon_1 < \varepsilon_4 - \varepsilon_3 < \varepsilon_4,\ \varepsilon_4 \equiv \varepsilon_1 + \varepsilon_3 \pmod 2, \\ h_3 = \varepsilon' - \varepsilon_4,\ k_2 = \varepsilon_3,\ A = 2^{\varepsilon_4 - \varepsilon_3} A_1, \\ r_1 = 2^{(\varepsilon_4 - \varepsilon_1 - \varepsilon_3)/2} r_2,\ A_1 \equiv s_1 \pmod 2; \\ \text{if } \varepsilon_3 \geq 1, \text{ then } A_1 \equiv s_1 \equiv 1 \pmod 2; \\ c \equiv 0 \text{ or } 1 \pmod 2 \text{ according as } r_2 \\ \text{satisfies } \Omega_3 r_2^2 + A_1 \equiv 0 \text{ or } 2^{\varepsilon_3} \pmod{2^{\varepsilon_3 + 1}}. \end{cases}$$

If $\varepsilon_3 = 0$, then $\varepsilon_4 - \varepsilon_3 < \varepsilon_4 \Rightarrow \varepsilon_4 < \varepsilon_4$, which is absurd, and thus $P^{(1)}_{ab}$, $P^{(1)}_{ac}$, $P^{(1)}_{ar}$ and $P^{(1)}_{as}$ are not satisfied. $\varepsilon_1 + \varepsilon_4 = 0$ is impossible since $\varepsilon_1 < \varepsilon_4 - \varepsilon_3 < \varepsilon_4 \Rightarrow \varepsilon_1 < \varepsilon_4$, and thus $P^{(2)}_{ab}$, $P^{(1)}_{bc}$, $P^{(1)}_{br}$ and $P^{(1)}_{bs}$ are not satisfied. If $\varepsilon_1 + n_2 = 0$, then $\varepsilon_1 = n_2 = 0$. Now $n_2 = 0 \Rightarrow r_1$ is odd. But $r_1 = 2^{(\varepsilon_4 - \varepsilon_1 - \varepsilon_3)/2} r_2$ and r_1 odd $\Rightarrow r_2$ odd and $\varepsilon_1 = \varepsilon_4 - \varepsilon_3$, which is impossible since $\varepsilon_1 < \varepsilon_4 - \varepsilon_3$ and thus $P^{(2)}_{ar}$, $P^{(2)}_{br}$, $P^{(2)}_{cr}$ and $P^{(1)}_{rs}$ are not satisfied. If $n_1 = 0$, then each of $P^{(2)}_{as}$, $P^{(2)}_{bs}$, $P^{(2)}_{cs}$ and $P^{(2)}_{rs}$ is satisfied according as $D = 1$, $(\Omega_1, Ds_1') = (b_2, s_1') = 1$, $(c', Ds_1') = 1$ and $(\Omega_1 r_1', Ds_1') = 1$.

Further, the existing primitive form is properly primitive iff c is odd.

Subcase (iii)$_{2211}$

$$\begin{cases} \epsilon_4 - \epsilon_3 \le \epsilon_1 < \epsilon_4,\ \epsilon_3 > \epsilon_2,\ \epsilon_4 \equiv \epsilon' \ (\text{mod } 2), \\ h_1 = \epsilon_3 - \epsilon_2,\ k_2 = \epsilon_4 - \epsilon_1,\ A = 2^{\epsilon_1}A_2, \\ s_1 = 2^{(\epsilon'-\epsilon_4)/2}s_2,\ s_2A_2r_1 \text{ odd, } c \equiv 0 \\ \text{or } 1 \ (\text{mod } 2) \text{ according as } r_1 \text{ satisfies} \\ \Omega_3 r_1^2 + A_2 \equiv 0 \text{ or } 2^{\epsilon_4-\epsilon_1}\ (\text{mod } 2^{\epsilon_4-\epsilon_1+1}). \end{cases}$$

If $\epsilon_3 = 0$, then $\epsilon_3 > \epsilon_2 \Rightarrow \epsilon_2 < 0$, which is impossible, and thus $P^{(1)}_{ab}$, $P^{(1)}_{ac}$, $P^{(1)}_{ar}$ and $P^{(1)}_{as}$ are not satisfied. $\epsilon_1 + \epsilon_4 = 0$ is impossible since $\epsilon_1 < \epsilon_4$, and thus $P^{(2)}_{ab}$, $P^{(1)}_{bc}$, $P^{(1)}_{br}$ and $P^{(1)}_{bs}$ are not satisfied. If $\epsilon_1 + n_2 = 0$, then $\epsilon_1 = n_2 = 0$. Now $\epsilon_1 = 0$ and $\epsilon_3 \le \epsilon_4 < \epsilon' = \epsilon_1 + \epsilon_2$ $\Rightarrow \epsilon_3 < \epsilon_2$, which is impossible since $\epsilon_3 > \epsilon_2$, and thus $P^{(2)}_{ar}$, $P^{(2)}_{br}$, $P^{(2)}_{cr}$ and $P^{(1)}_{rs}$ are not satisfied. If $n_1 = 0$, then s_1 is odd. But $s_1 = 2^{(\epsilon'-\epsilon_4)/2}s_2$ and s_1 odd $\Rightarrow s_2$ odd and $\epsilon' = \epsilon_4$, which is impossible since $\epsilon_4 < \epsilon'$, and thus $P^{(2)}_{as}$, $P^{(2)}_{bs}$, $P^{(2)}_{cs}$ and $P^{(2)}_{rs}$ are not satisfied. Moreover, the existing primitive form is properly primitive.

Subcase (iii)$_{2221}$

$$\begin{cases} \epsilon_4 - \epsilon_3 \le \epsilon_1 < \epsilon_4,\ \epsilon_3 \le \epsilon_2,\ \epsilon_4 \equiv \epsilon_1 + \epsilon_3 \\ (\text{mod } 2),\ \ h_3 = \epsilon_2 - \epsilon_3,\ k_2 = \epsilon_4 - \epsilon_1, \\ A = 2^{\epsilon_1}A_2,\ s_1 = 2^{(\epsilon_1-\epsilon_4+\epsilon_3)/2}s_2,\ A_2s_2r_1 \end{cases}$$

Subcase (iii)$_{2221}$ continued

odd if $\varepsilon_3 < \varepsilon_2$; if $\varepsilon_3 = \varepsilon_2$, then
$A_2 r_1 \equiv s_2 + 1 \equiv 1 \pmod{2}$ or
$(A_2/4)(r_1/2)s_2 \equiv 1 \pmod{2}$; $c \equiv 0$
or $1 \pmod{2}$ according as r_1 satisfies
$\Omega_3 r_1^2 + A_2 \equiv 0$ or $2^{\varepsilon_4 - \varepsilon_1} \pmod{2^{\varepsilon_4 - \varepsilon_1 + 1}}$.

If $\varepsilon_3 = 0$, then $\varepsilon_4 - \varepsilon_3 \leq \varepsilon_1 < \varepsilon_4 \Rightarrow \varepsilon_4 < \varepsilon_4$, which is absurd, and thus $P_{ab}^{(1)}$, $P_{ac}^{(1)}$, $P_{ar}^{(1)}$ and $P_{as}^{(1)}$ are not satisfied. $\varepsilon_1 + \varepsilon_4 = 0$ is impossible since $\varepsilon_1 < \varepsilon_4$, and thus $P_{ab}^{(2)}$, $P_{bc}^{(1)}$, $P_{br}^{(1)}$ and $P_{bs}^{(1)}$ are not satisfied. If $\varepsilon_1 + n_2 = 0$, then each of $P_{ar}^{(2)}$, $P_{br}^{(2)}$, $P_{cr}^{(2)}$ and $P_{rs}^{(1)}$ is satisfied according as $(a_1, r_1') = (D, \Omega_1) = 1$, $\Omega_1 = (b_2, r_1') = 1$, $(c', \Omega_1 r_1') = 1$ and $(\Omega_1 r_1', Ds_1') = 1$. If $n_1 = 0$, then each of $P_{as}^{(2)}$, $P_{bs}^{(2)}$, $P_{cs}^{(2)}$ and $P_{rs}^{(2)}$ is satisfied according as $D = 1$, $(\Omega_1, Ds_1') = (b_2, s_1') = 1$, $(c', Ds_1') = 1$ and $(\Omega_1 r_1', Ds_1') = 1$. Further, the existing primitive form is properly primitive iff c is odd.

Subcase (iii)$_{2222}$

$\varepsilon_4 - \varepsilon_3 \leq \varepsilon_1 < \varepsilon_4$, $\varepsilon_3 = \varepsilon_2$, $\varepsilon_4 \equiv \varepsilon_1 + \varepsilon_3$
$+ 1 \pmod{2}$, $h_2 = 1$, $k_2 = \varepsilon_4 - \varepsilon_1$,
$A = 2^{\varepsilon_1} A_2$, $s_1 = 2^{(\varepsilon_1 - \varepsilon_4 + \varepsilon_3 + 1)/2} s_2$,
$A_2 r_1 \equiv 1 \pmod{2}$, $c \equiv 0$ or $1 \pmod{2}$
according as r_1 satisfies $\Omega_3 r_1^2 + A_2 \equiv 0$
or $2^{\varepsilon_4 - \varepsilon_1} \pmod{2^{\varepsilon_4 - \varepsilon_1 + 1}}$.

If $\varepsilon_3 = 0$, then $\varepsilon_4 - \varepsilon_3 \leq \varepsilon_1 < \varepsilon_4 \Rightarrow \varepsilon_4 < \varepsilon_4$, which is absurd and thus *$P_{ab}^{(1)}$, $P_{ac}^{(1)}$, $P_{ar}^{(1)}$ and $P_{as}^{(1)}$ are not satisfied.* $\varepsilon_1 + \varepsilon_4 = 0$ is impossible since $\varepsilon_1 < \varepsilon_4$, and thus *$P_{ab}^{(2)}$, $P_{bc}^{(1)}$, $P_{br}^{(1)}$ and $P_{bs}^{(1)}$ are not satisfied.* If $\varepsilon_1 + n_2 = 0$, then $\varepsilon_1 = n_2 = 0$. But $\varepsilon_1 = 0$ and $\varepsilon_3 \leq \varepsilon_4 < \varepsilon' = \varepsilon_1 + \varepsilon_2 \Rightarrow \varepsilon_3 < \varepsilon_2$, which is impossible since $\varepsilon_3 = \varepsilon_2$, and thus *$P_{ar}^{(2)}$, $P_{br}^{(2)}$, $P_{cr}^{(2)}$ and $P_{rs}^{(1)}$ are not satisfied.* If $n_1 = 0$, then s_1 is odd. But $s_1 = 2^{(\varepsilon_1 - \varepsilon_4 + \varepsilon_3 + 1)/2} s_2$ and s_1 odd $\Rightarrow s_2$ odd and $\varepsilon_4 - \varepsilon_3 = \varepsilon_1 + 1$, that is, $\varepsilon_4 - \varepsilon_3 > \varepsilon_1$, which is impossible since $\varepsilon_4 - \varepsilon_3 \leq \varepsilon_1$, and thus *$P_{as}^{(2)}$, $P_{bs}^{(2)}$, $P_{cs}^{(2)}$ and $P_{rs}^{(2)}$ are not satisfied.* Moreover, the existing primitive form is properly primitive.

Case (iv) $\varepsilon_4 < \varepsilon_3 < \varepsilon'$:

If $\varepsilon_3 = 0$, then $\varepsilon_4 < \varepsilon_3 \Rightarrow \varepsilon_4 < 0$, which is impossible, and thus *$P_{ab}^{(1)}$, $P_{ac}^{(1)}$, $P_{ar}^{(1)}$ and $P_{as}^{(1)}$ are not satisfied in any subcase of (iv).*

Subcase $(\text{iv})_{1311}$ $\left\{\right.$ *$\varepsilon_4 \leq \varepsilon_1$, $\varepsilon_4 \equiv \varepsilon_3 \pmod 2$, $\varepsilon_4 \geq \varepsilon_5$, $\varepsilon_5 \equiv 0 \pmod 2$*, $h_1 = \varepsilon_4 - \varepsilon_5$, $k_3 = \varepsilon_1 - \varepsilon_4$, $A = 2^{\varepsilon_4} A_1$, $s_1 = 2^{(\varepsilon' - \varepsilon_4)/2} s_3$, $A_1 \equiv 0$ or $1 \pmod 2$ according as s_3 is chosen to

Subcase $(iv)_{1311}$ continued

satisfy $b_2D_2s_3^2 + \delta_2 \equiv 0$ or $2^{\epsilon_4-\epsilon_5}$ (mod $2^{\epsilon_4-\epsilon_5+1}$), $c \equiv A_1 + 2^{\epsilon_1-\epsilon_4}r_1$ (mod 2).

If $\epsilon_1 + \epsilon_4 = 0$, then $\epsilon_4 \geq \epsilon_5 = \epsilon' - \epsilon_3 = \epsilon_1 + \epsilon_2 - \epsilon_3$ $\Rightarrow \epsilon_3 \geq \epsilon_2$, which is impossible since $\epsilon_4 < \epsilon_3 \leqslant \epsilon' = \epsilon_1 + \epsilon_2$ $\Rightarrow 0 < \epsilon_3 < \epsilon_2$, and thus $P_{ab}^{(2)}$, $P_{bc}^{(1)}$, $P_{br}^{(1)}$ and $P_{bs}^{(1)}$ are not satisfied. If $\epsilon_1 + n_2 = 0$, then $\epsilon_1 = n_2 = 0$. $\epsilon_1 = 0$ and $\epsilon_4 \leq \epsilon_1 \Rightarrow \epsilon_4 = 0$, which is impossible by the previous argument, and thus $P_{ar}^{(2)}$, $P_{br}^{(2)}$, $P_{cr}^{(2)}$ and $P_{rs}^{(1)}$ are not satisfied. If $n_1 = 0$, then s_1 is odd. But $s_1 = 2^{(\epsilon'-\epsilon_4)/2} s_3$ and s_1 odd $\Rightarrow s_3$ odd and $\epsilon_4 = \epsilon'$, which is impossible since $\epsilon_4 < \epsilon'$, and thus $P_{as}^{(2)}$, $P_{bs}^{(2)}$, $P_{cs}^{(2)}$ and $P_{rs}^{(2)}$ are not satisfied. Furthermore, the existing primitive form is properly primitive.

Subcase $(iv)_{1312}$

$$\begin{cases} \epsilon_4 \leq \epsilon_1,\ \epsilon_4 \equiv \epsilon_3 \pmod 2,\ \epsilon_4 = \epsilon_5, \\ \epsilon_5 \equiv 1 \pmod 2,\ h_2 = 1,\ k_3 = \epsilon_3 - \epsilon_2, \\ A = 2^{\epsilon_4}A_1,\ s_1 = 2^{(\epsilon_3+1)/2} s_3,\ A_1 \text{ odd}, \\ c \equiv 1 + 2^{\epsilon_3-\epsilon_2}r_1 \pmod 2. \end{cases}$$

If $\epsilon_1 + \epsilon_4 = 0$, then $\epsilon_4 = \epsilon_5 \Rightarrow \epsilon_5 = 0$, which is impossible since $\epsilon_5 \equiv 1$ (mod 2), and thus $P_{ab}^{(2)}$, $P_{bc}^{(1)}$, $P_{br}^{(1)}$ and $P_{bs}^{(1)}$ are not satisfied. If $\epsilon_1 + n_2 = 0$, then $\epsilon_1 = n_2 = 0$. Now $\epsilon_1 = 0$ and $\epsilon_4 \leq \epsilon_1 \Rightarrow \epsilon_4 = 0$, which is impossible by the preceding argument, and thus $P^{(2)}_{ar}$, $P^{(2)}_{br}$, $P^{(2)}_{cr}$ and $P^{(1)}_{rs}$ are not satisfied. If $n_1 = 0$, then s_1 is odd. But $s_1 = 2^{(\varepsilon_3+1)/2} s_3$ and s_1 odd $\Rightarrow$ s_3 odd and $\varepsilon_3 + 1 = 0$, which is impossible since ε_3 is non-negative, and thus $P^{(2)}_{as}$, $P^{(2)}_{bs}$, $P^{(2)}_{cs}$ and $P^{(2)}_{rs}$ are not satisfied. Moreover, the existing primitive form is properly primitive.

Subcase $(iv)_{1321}$

$$\begin{cases} \varepsilon_4 \leq \varepsilon_1,\ 0 \equiv \varepsilon_4 \equiv \varepsilon_3 \pmod 2,\ \varepsilon_4 < \varepsilon_5, \\ h_3 = \varepsilon_5 - \varepsilon_4,\ k_3 = \varepsilon_1 - \varepsilon_4,\ A = 2^{\varepsilon_4} A_1, \\ s_1 = 2^{\varepsilon_3/2} s_3,\ A_1 \equiv s_3 \equiv 1 \pmod 2, \\ c \equiv 1 + 2^{\varepsilon_1 - \varepsilon_4} r_1 \pmod 2. \end{cases}$$

If $\varepsilon_1 + \varepsilon_4 = 0$, then each of $P^{(2)}_{ab}$, $P^{(1)}_{bc}$, $P^{(1)}_{br}$ and $P^{(1)}_{bs}$ is satisfied according as $(D, \Omega_1) = 1$, $(\Omega_1 b_2, c') = 1$, $\Omega_1 = (b_2, r_1') = 1$ and $(\Omega_1, Ds_1') = (b_2, s_1') = 1$. If $\varepsilon_1 + n_2 = 0$, then each of $P^{(2)}_{ar}$, $P^{(2)}_{br}$, $P^{(2)}_{cr}$ and $P^{(1)}_{rs}$ is satisfied according as $(a_1, r_1') = (D, \Omega_1) = 1$, $\Omega_1 = (b_2, r_1') = 1$, $(c', \Omega_1 r_1') = 1$ and $(\Omega_1 r_1', Ds_1') = 1$. If $n_1 = 0$, then s_1 is odd. But $s_1 = 2^{\varepsilon_3/2} s_3$, s_1 odd and s_3 odd $\Rightarrow$ $\varepsilon_3 = 0$, which is impossible since $\varepsilon_3 = 0$ and $\varepsilon_4 < \varepsilon_3 \Rightarrow \varepsilon_4 < 0$, and thus $P^{(2)}_{as}$, $P^{(2)}_{bs}$, $P^{(2)}_{cs}$ and $P^{(2)}_{rs}$ are not satisfied. Further, the existing primitive form is properly primitive iff b or c is odd.

Subcase $(\mathrm{iv})_{13221}$
$$\begin{cases} \varepsilon_4 = \varepsilon_1,\ 1 \equiv \varepsilon_4 \equiv \varepsilon_3 \pmod 2,\ \varepsilon_4 < \varepsilon_5, \\ h_3 = (\varepsilon_5 - 1) - \varepsilon_4,\ k_1 = 1,\ A = 2^{\varepsilon_4+1} A_2, \\ s_1 = 2^{(\varepsilon_3+1)/2} s_3,\ A_2 \equiv s_3 + 2^{(\varepsilon_5-1)-\varepsilon_4} \\ \pmod 2,\ c \equiv r_1 \pmod 2. \end{cases}$$

If $\varepsilon_1 + \varepsilon_4 = 0$, then $\varepsilon_1 = \varepsilon_4 = 0$. But $\varepsilon_4 = 0$ is impossible since $\varepsilon_4 \equiv 1 \pmod 2$, and thus $P^{(2)}_{ab}$, $P^{(1)}_{bc}$, $P^{(1)}_{br}$ and $P^{(1)}_{bs}$ are not satisfied. If $\varepsilon_1 + n_2 = 0$, then $\varepsilon_1 = n_2 = 0$. But $\varepsilon_1 = 0$ and $\varepsilon_4 = \varepsilon_1 \Rightarrow \varepsilon_4 = 0$, which is impossible by the previous argument, and thus $P^{(2)}_{ar}$, $P^{(2)}_{br}$, $P^{(2)}_{cr}$ and $P^{(1)}_{rs}$ are not satisfied. If $n_1 = 0$, then s_1 is odd. But $s_1 = 2^{(\varepsilon_3+1)/2} s_3$ and s_1 odd $\Rightarrow s_3$ odd and $\varepsilon_3 + 1 = 0$, which is impossible since ε_3 is non-negative, and thus $P^{(2)}_{as}$, $P^{(2)}_{bs}$, $P^{(2)}_{cs}$ and $P^{(2)}_{rs}$ are not satisfied. Further, the existing primitive form is properly primitive.

Subcase $(\mathrm{iv})_{13222}$
$$\begin{cases} \varepsilon_4 < \varepsilon_1,\ 1 \equiv \varepsilon_4 \equiv \varepsilon_3 \pmod 2,\ \varepsilon_4 < \varepsilon_5, \\ h_3 = (\varepsilon_5 - 1) - \varepsilon_4,\ k_3 = (\varepsilon_1 - 1) - \varepsilon_4, \\ A = 2^{\varepsilon_4+1} A_2,\ s_1 = 2^{(\varepsilon_3+1)/2} s_3,\ c = 2c_1, \\ A_2 \equiv s_3 + 2^{(\varepsilon_5-1)-\varepsilon_4} \pmod 2, \\ c_1 \equiv A_2 + 2^{(\varepsilon_1-1)-\varepsilon_4} r_1 \pmod 2. \end{cases}$$

$\varepsilon_1 + \varepsilon_4 = 0$ is impossible since $\varepsilon_4 < \varepsilon_1$, and thus $P^{(2)}_{ab}$, $P^{(1)}_{bc}$, $P^{(1)}_{br}$ and $P^{(1)}_{bs}$ are not satisfied. If $n_3 = 0$, then c is odd, which is impossible since $c = 2c_1$, and thus $P^{(2)}_{ac}$, $P^{(2)}_{bc}$, $P^{(1)}_{cr}$ and $P^{(1)}_{cs}$ are not satisfied. If $\epsilon_1 + n_2 = 0$, then $\epsilon_1 = n_2 = 0$. But $\epsilon_1 = 0$ and $\epsilon_4 < \epsilon_1 \Rightarrow \epsilon_4 < 0$, which is impossible, and thus $P^{(2)}_{ar}$, $P^{(2)}_{br}$, $P^{(2)}_{cr}$ and $P^{(1)}_{rs}$ are not satisfied. If $n_1 = 0$, then s_1 is odd. But $s_1 = 2^{(\epsilon_3+1)/2} s_3$ and s_1 odd $\Rightarrow$ s_3 odd and $\epsilon_3 + 1 = 0$, which is impossible since ϵ_3 is non-negative, and thus $P^{(2)}_{as}$, $P^{(2)}_{bs}$, $P^{(2)}_{cs}$ and $P^{(2)}_{rs}$ are not satisfied. Hence, a primitive form does not exist in this subcase.

Subcase $(iv)_{1411}$

$$\left\{\begin{array}{l}
\epsilon_4 \le \epsilon_1,\ \epsilon_4 \equiv \epsilon_3 + 1 \pmod 2, \\
1 \le \epsilon_5 \le \epsilon_4,\ \epsilon_5 \equiv 1 \pmod 2,\quad h_1 = \epsilon_4 - \epsilon_5, \\
k_3 = \epsilon_1 - \epsilon_4,\ A = 2^{\epsilon_4} A_2,\ s_1 = 2^{(\epsilon' - \epsilon_4)/2} s_3, \\
s_3 \text{ odd if } \epsilon_5 < \epsilon_4,\ A_2 \equiv 0 \text{ or } 1 \pmod 2 \\
\text{according as } s_3 \text{ satisfies } b_2 D_2 s_3^2 + \delta_2 \equiv 0 \\
\text{or } 2^{\epsilon_4 - \epsilon_5} \pmod{2^{\epsilon_4 - \epsilon_5 + 1}}, \\
c \equiv A_2 + 2^{\epsilon_1 - \epsilon_4} r_1 \pmod 2.
\end{array}\right.$$

If $\epsilon_1 + \epsilon_4 = 0$, then $1 \le \epsilon_5 = \epsilon' - \epsilon_3 = \epsilon_1 + \epsilon_2 - \epsilon_3 \le \epsilon_4 \Rightarrow 1 \le \epsilon_2 - \epsilon_3 \le 0$, which is absurd, and thus $P^{(2)}_{ab}$, $P^{(1)}_{bc}$, $P^{(1)}_{br}$ and $P^{(1)}_{bs}$ are not satisfied. If $\epsilon_1 + n_2 = 0$, then $\epsilon_1 = n_2 = 0$. But $\epsilon_1 = 0$ and $\epsilon_4 \le \epsilon_1 \Rightarrow \epsilon_4 = 0$, which is impossible by the preceding argument, and thus $P^{(2)}_{ar}$, $P^{(2)}_{br}$, $P^{(2)}_{cr}$

and $P_{rs}^{(1)}$ are not satisfied. If $n_1 = 0$, then s_1 is odd. But $s_1 = 2^{(\epsilon'-\epsilon_4)/2} s_3$ and s_1 odd $\Rightarrow$ s_3 odd and $\epsilon_4 = \epsilon'$, which is impossible since $\epsilon_4 < \epsilon'$, and thus *$P_{as}^{(2)}$, $P_{bs}^{(2)}$, $P_{cs}^{(2)}$ and $P_{rs}^{(2)}$ are not satisfied.* Furthermore, the existing primitive form is properly primitive.

Subcase $(\text{iv})_{1412}$

$$\left\{\begin{array}{l} \epsilon_4 \le \epsilon_1,\ \epsilon_4 \equiv \epsilon_3 + 1 \pmod{2},\ 1 \le \epsilon_5 \\ = \epsilon_4,\ \epsilon_5 \equiv 0 \pmod{2},\ h_2 = 1,\ k_3 = \epsilon_1 - \epsilon_4, \\ A = 2^{\epsilon_4} A_2,\ s_1 = 2^{(\epsilon'-\epsilon_4+1)/2} s_3,\ A_2 \text{ odd}, \\ c \equiv 1 + 2^{\epsilon_1-\epsilon_4} r_1 \pmod{2}. \end{array}\right.$$

If $\epsilon_1 + \epsilon_4 = 0$, then $1 \le \epsilon_5 = \epsilon' - \epsilon_3 = \epsilon_1 + \epsilon_2 - \epsilon_3 = \epsilon_4 \Rightarrow 1 \le \epsilon_2 - \epsilon_3 = 0$, which is absurd, and thus *$P_{ab}^{(2)}$, $P_{bc}^{(1)}$, $P_{br}^{(1)}$ and $P_{bs}^{(1)}$ are not satisfied.* If $\epsilon_1 + n_2 = 0$, then $\epsilon_1 = n_2 = 0$. But $\epsilon_1 = 0$ and $\epsilon_4 \le \epsilon_1 \Rightarrow \epsilon_4 = 0$, which is impossible since $\epsilon_4 \ge 1$, and thus *$P_{ar}^{(2)}$, $P_{br}^{(2)}$, $P_{cr}^{(2)}$ and $P_{rs}^{(1)}$ are not satisfied.* If $n_1 = 0$, then s_1 is odd. But $s_1 = 2^{(\epsilon'-\epsilon_4+1)/2} s_3$ and s_1 odd $\Rightarrow$ s_3 odd and $\epsilon_4 = \epsilon' + 1 > \epsilon'$, which is impossible since $\epsilon_4 < \epsilon'$, and thus *$P_{as}^{(2)}$, $P_{bs}^{(2)}$, $P_{cs}^{(2)}$ and $P_{rs}^{(2)}$ are not satisfied.* Furthermore, the existing primitive form is properly primitive.

Subcase (iv)$_{1421}$

$$\begin{cases} \epsilon_4 \le \epsilon_1,\ 1 \le \epsilon_4 < \epsilon_5,\ 1 \equiv \epsilon_4 \equiv \epsilon_3 + 1 \\ (\text{mod } 2),\ h_3 = \epsilon_5 - \epsilon_4,\ k_3 = \epsilon_1 - \epsilon_4, \\ A = 2^{\epsilon_4} A_2,\ s_1 = 2^{\epsilon_3/2} s_3,\ A_2 s_3 \text{ odd}, \\ c \equiv 1 + 2^{\epsilon_1 - \epsilon_4} r_1 \ (\text{mod } 2). \end{cases}$$

If $\epsilon_1 + \epsilon_4 = 0$, then $\epsilon_1 = \epsilon_4 = 0$. But $\epsilon_4 = 0$ is impossible since $\epsilon_4 \ge 1$, and thus $P_{ab}^{(2)}$, $P_{bc}^{(1)}$, $P_{br}^{(1)}$ and $P_{bs}^{(1)}$ are not satisfied. If $\epsilon_1 + n_2 = 0$, then $\epsilon_1 = n_2 = 0$. But $\epsilon_1 = 0$ and $\epsilon_4 \le \epsilon_1 \Rightarrow \epsilon_4 = 0$, which is impossible since $\epsilon_4 \ge 1$, and thus $P_{ar}^{(2)}$, $P_{br}^{(2)}$, $P_{cr}^{(2)}$ and $P_{rs}^{(1)}$ are not satisfied. If $n_1 = 0$, then s_1 is odd. But $s_1 = 2^{\epsilon_3/2} s_3$, s_1 odd and s_3 odd $\Rightarrow \epsilon_3 = 0$, which is impossible since $\epsilon_3 = 0$ and $\epsilon_4 < \epsilon_3 \Rightarrow \epsilon_4 < 0$, and thus $P_{as}^{(2)}$, $P_{bs}^{(2)}$, $P_{cs}^{(2)}$ and $P_{rs}^{(2)}$ are not satisfied. Moreover, the existing primitive form is properly primitive.

Subcase (iv)$_{14221}$

$$\begin{cases} \epsilon_4 = \epsilon_1,\ 1 \le \epsilon_4 < \epsilon_5,\ 0 \equiv \epsilon_4 \equiv \epsilon_3 + 1 \\ (\text{mod } 2),\ h_3 = (\epsilon_5 - 1) - \epsilon_4,\ k_1 = 1, \\ A = 2^{\epsilon_4 + 1} A_3,\ s_1 = 2^{(\epsilon_3 + 1)/2} s_3, \\ A_3 \equiv s_3 + 2^{(\epsilon_5 - 1) - \epsilon_4} \ (\text{mod } 2), \\ c \equiv r_1 \ (\text{mod } 2). \end{cases}$$

If $\epsilon_1 + \epsilon_4 = 0$, then $\epsilon_1 = \epsilon_4 = 0$. But $\epsilon_4 = 0$ is impossible since $\epsilon_4 \ge 1$, and thus $P_{ab}^{(2)}$, $P_{bc}^{(1)}$, $P_{br}^{(1)}$ and $P_{bs}^{(1)}$

are not satisfied. If $\varepsilon_1 + n_2 = 0$, then $\varepsilon_1 = n_2 = 0$. But $\varepsilon_1 = 0$ and $\varepsilon_4 = \varepsilon_1 \Rightarrow \varepsilon_4 = 0$, which is impossible since $\varepsilon_4 \geq 1$, and thus $P^{(2)}_{ar}$, $P^{(2)}_{br}$, $P^{(2)}_{cr}$ and $P^{(1)}_{rs}$ are not satisfied. If $n_1 = 0$, then s_1 is odd. But $s_1 = 2^{(\varepsilon_3+1)/2} s_3$ and s_1 odd $\Rightarrow$ s_3 odd and $\varepsilon_3 + 1 = 0$, which is impossible since ε_3 is non-negative, and thus $P^{(2)}_{as}$, $P^{(2)}_{bs}$, $P^{(2)}_{cs}$ and $P^{(2)}_{rs}$ are not satisfied. Further, the existing primitive form is properly primitive.

Subcase $(\text{iv})_{14222}$
$$\left\{\begin{array}{l}
\varepsilon_4 < \varepsilon_1,\ 1 \leq \varepsilon_4 < \varepsilon_5,\ 0 \equiv \varepsilon_4 \equiv \varepsilon_3 + 1 \\
(\text{mod } 2),\quad h_3 = (\varepsilon_5 - 1) - \varepsilon_4, \\
k_3 = (\varepsilon_1 - 1) - \varepsilon_4,\ A = 2^{\varepsilon_4+1} A_3, \\
s_1 = 2^{(\varepsilon_3+1)/2} s_3,\ c = 2c_1, \\
A_3 \equiv s_3 + 2^{(\varepsilon_5-1)-\varepsilon_4} \pmod 2, \\
c_1 \equiv A_3 + 2^{(\varepsilon_1-1)-\varepsilon_4} r_1 \pmod 2.
\end{array}\right.$$

$\varepsilon_1 + \varepsilon_4 = 0$ is impossible since $\varepsilon_4 < \varepsilon_1$, and thus $P^{(2)}_{ab}$, $P^{(1)}_{bc}$, $P^{(1)}_{br}$ and $P^{(1)}_{bs}$ are not satisfied. If $n_3 = 0$, then c is odd, which is impossible since $c = 2c_1$, and thus $P^{(2)}_{ac}$, $P^{(2)}_{bc}$, $P^{(1)}_{cr}$ and $P^{(1)}_{cs}$ are not satisfied. If $\varepsilon_1 + n_2 = 0$, then $\varepsilon_1 = n_2 = 0$. But $\varepsilon_1 = 0$ and $\varepsilon_4 < \varepsilon_1 \Rightarrow \varepsilon_4 < 0$, which is impossible, and thus $P^{(2)}_{ar}$, $P^{(2)}_{br}$, $P^{(2)}_{cr}$ and $P^{(1)}_{rs}$ are not satisfied. If $n_1 = 0$, then s_1 is odd. But $s_1 = 2^{(\varepsilon_3+1)/2} s_3$

and s_1 odd $\Rightarrow s_3$ odd and $\varepsilon_3 + 1 = 0$, which is impossible since ε_3 is non-negative, and thus $P^{(2)}_{as}$, $P^{(2)}_{bs}$, $P^{(2)}_{cs}$ and $P^{(2)}_{rs}$ are not satisfied. Hence, a primitive form does not exist in this subcase.

Subcase $(iv)_{2311}$ $\left\{\right.$ $\varepsilon_4 > \varepsilon_1$, $\varepsilon_4 \equiv \varepsilon_3 \pmod 2$, $\varepsilon_3 \geq \varepsilon_2$, $\varepsilon_5 \equiv 0 \pmod 2$, $h_1 = \varepsilon_3 - \varepsilon_2$, $k_2 = \varepsilon_4 - \varepsilon_1$, $A = 2^{\varepsilon_1}A_1$, $s_1 = 2^{(\varepsilon' - \varepsilon_4)/2} s_3$, $s_3A_1r_1$ odd if $\varepsilon_3 > \varepsilon_2$; $A_1r_1 \equiv s_3 + 1 \equiv 1 \pmod 2$ or $(A_1/4)(r_1/2)s_3 \equiv 1 \pmod 2$ if $\varepsilon_3 = \varepsilon_2$; $c \equiv 0$ or $1 \pmod 2$ according as r_1 satisfies $\Omega_3 r_1^2 + A_1 \equiv 0$ or $2^{\varepsilon_4 - \varepsilon_1} \pmod{2^{\varepsilon_4 - \varepsilon_1 + 1}}$.

$\varepsilon_1 + \varepsilon_4 = 0$ is impossible since $\varepsilon_4 > \varepsilon_1$, and thus $P^{(2)}_{ab}$, $P^{(1)}_{bc}$, $P^{(1)}_{br}$ and $P^{(1)}_{bs}$ are not satisfied. If $\varepsilon_1 + n_2 = 0$, then $\varepsilon_1 = n_2 = 0$. But $\varepsilon_1 = 0$ and $\varepsilon_3 < \varepsilon' = \varepsilon_1 + \varepsilon_2 \Rightarrow \varepsilon_3 < \varepsilon_2$, which is impossible since $\varepsilon_3 \geq \varepsilon_2$, and thus $P^{(2)}_{ar}$, $P^{(2)}_{br}$, $P^{(2)}_{cr}$ and $P^{(1)}_{rs}$ are not satisfied. If $n_1 = 0$, then s_1 is odd. But $s_1 = 2^{(\varepsilon' - \varepsilon_4)/2} s_3$ and s_1 odd $\Rightarrow s_3$ odd and $\varepsilon_4 = \varepsilon'$, which is impossible since $\varepsilon_4 < \varepsilon'$, and thus $P^{(2)}_{as}$, $P^{(2)}_{bs}$, $P^{(2)}_{cs}$ and $P^{(2)}_{rs}$ are not satisfied. Furthermore, the existing primitive form is properly primitive.

Subcase (iv)$_{2312}$

$$\left\{\begin{array}{l} \epsilon_4 > \epsilon_1,\ \epsilon_4 \equiv \epsilon_3 \pmod 2,\ \epsilon_3 = \epsilon_2, \\ \epsilon_5 \equiv 1 \pmod 2,\ h_2 = 1,\ k_2 = \epsilon_4 - \epsilon_1, \\ A = 2^{\epsilon_1}A_1,\ s_1 = 2^{(\epsilon'-\epsilon_4+1)/2}s_3,\ A_1r_1 \\ \text{odd, } c \equiv 0 \text{ or } 1 \pmod 2 \text{ according as } r_1 \\ \text{satisfies } \Omega_3r_1^2 + A_1 \equiv 0 \text{ or } 2^{\epsilon_4-\epsilon_1} \\ (\mathrm{mod}\ 2^{\epsilon_4-\epsilon_1+1}). \end{array}\right.$$

$\epsilon_1 + \epsilon_4 = 0$ is impossible since $\epsilon_4 > \epsilon_1$, and thus $P^{(2)}_{ab}$, $P^{(1)}_{bc}$, $P^{(1)}_{br}$ and $P^{(1)}_{bs}$ are not satisfied. If $\epsilon_1 + n_2 = 0$, then $\epsilon_1 = n_2 = 0$. But $\epsilon_1 = 0$ and $\epsilon_3 < \epsilon' = \epsilon_1 + \epsilon_2 \Rightarrow \epsilon_3 < \epsilon_2$, which is impossible since $\epsilon_3 = \epsilon_2$, and thus $P^{(2)}_{ar}$, $P^{(2)}_{br}$, $P^{(2)}_{cr}$ and $P^{(1)}_{rs}$ are not satisfied. If $n_1 = 0$, then s_1 is odd. But $s_1 = 2^{(\epsilon'-\epsilon_4+1)/2}s_3$ and s_1 odd $\Rightarrow$ s_3 odd and $\epsilon_4 = \epsilon' + 1 > \epsilon'$, which is impossible since $\epsilon_4 < \epsilon'$, and thus $P^{(2)}_{as}$, $P^{(2)}_{bs}$, $P^{(2)}_{cs}$ and $P^{(2)}_{rs}$ are not satisfied. Moreover, the existing primitive form is properly primitive.

Subcase (iv)$_{2321}$

$$\left\{\begin{array}{l} \epsilon_4 > \epsilon_1,\ \epsilon_4 \equiv \epsilon_3 \pmod 2,\ \epsilon_3 < \epsilon_2, \\ \epsilon_1 \equiv 0 \pmod 2,\ h_3 = \epsilon_2 - \epsilon_3,\ k_2 = \epsilon_4 - \epsilon_1, \\ A = 2^{\epsilon_1}A_1,\ s_1 = 2^{(\epsilon_1+\epsilon_3-\epsilon_4)/2}s_3,\ s_3A_1r_1 \\ \text{odd, } c \equiv 0 \text{ or } 1 \pmod 2 \text{ according as } r_1 \\ \text{satisfies } \Omega_3r_1^2 + A_1 \equiv 0 \text{ or } 2^{\epsilon_4-\epsilon_1} \\ (\mathrm{mod}\ 2^{\epsilon_4-\epsilon_1+1}). \end{array}\right.$$

$\epsilon_1 + \epsilon_4 = 0$ is impossible since $\epsilon_4 > \epsilon_1$, and thus $P^{(2)}_{ab}$, $P^{(1)}_{bc}$, $P^{(1)}_{br}$ and $P^{(1)}_{bs}$ are not satisfied. If $\epsilon_1 + n_2 = 0$, then each of $P^{(2)}_{ar}$, $P^{(2)}_{br}$, $P^{(2)}_{cr}$ and $P^{(1)}_{rs}$ is satisfied according as $(a_1, r_1') = (D, \Omega_1) = 1$, $\Omega_1 = (b_2, r_1') = 1$, $(c', \Omega_1 r_1') = 1$ and $(\Omega_1 r_1', Ds_1') = 1$. If $n_1 = 0$, then s_1 is odd. But $s_1 = 2^{(\epsilon_1+\epsilon_3-\epsilon_4)/2} s_3$, s_1 odd and s_3 odd $\Rightarrow \epsilon_4 = \epsilon_1 + \epsilon_3 \geq \epsilon_3$, which is impossible since $\epsilon_4 < \epsilon_3$, and thus $P^{(2)}_{as}$, $P^{(2)}_{bs}$, $P^{(2)}_{cs}$ and $P^{(2)}_{rs}$ are not satisfied. Further, the existing primitive form is properly primitive iff c is odd.

Subcase (iv)$_{2411}$

$$\left\{\begin{array}{l} \epsilon_4 > \epsilon_1 \geq 1,\ \epsilon_4 \equiv \epsilon_3 + 1 \pmod{2},\ \epsilon_3 \geq \epsilon_2, \\ \epsilon_5 \equiv 1 \pmod{2},\ h_1 = \epsilon_3 - \epsilon_2,\ k_2 = \epsilon_4 - \epsilon_1, \\ A = 2^{\epsilon_1} A_2,\ s_1 = 2^{(\epsilon' - \epsilon_4)/2} s_3,\ s_3 A_2 r_1 \text{ odd} \\ \text{if } \epsilon_3 > \epsilon_2;\ A_2 r_1 \equiv s_3 + 1 \equiv 1 \pmod{2} \text{ or} \\ (A_2/4)(r_1/2) s_3 \equiv 1 \pmod{2} \text{ if } \epsilon_3 = \epsilon_2; \\ c \equiv 0 \text{ or } 1 \pmod{2} \text{ according as } r_1 \\ \text{satisfies } \Omega_3 r_1^2 + A_2 \equiv 0 \text{ or } 2^{\epsilon_4 - \epsilon_1} \\ (\text{mod } 2^{\epsilon_4 - \epsilon_1 + 1}). \end{array}\right.$$

$\epsilon_1 + \epsilon_4 = 0$ is impossible since $\epsilon_4 > \epsilon_1$, and thus $P^{(2)}_{ab}$, $P^{(1)}_{bc}$, $P^{(1)}_{br}$ and $P^{(1)}_{bs}$ are not satisfied. If $\epsilon_1 + n_2 = 0$, then $\epsilon_1 = n_2 = 0$. But $\epsilon_1 = 0$ and $\epsilon_3 < \epsilon' = \epsilon_1 + \epsilon_2 \Rightarrow \epsilon_3 < \epsilon_2$, which is impossible since $\epsilon_3 \geq \epsilon_2$, and thus $P^{(2)}_{ar}$, $P^{(2)}_{br}$, $P^{(2)}_{cr}$

and $P^{(1)}_{rs}$ are not satisfied. If $n_1 = 0$, then s_1 is odd. But $s_1 = 2^{(\epsilon'-\epsilon_4)/2} \cdot s_3$ and s_1 odd $\Rightarrow$ s_3 odd and $\epsilon_4 = \epsilon'$, which is impossible since $\epsilon_4 < \epsilon'$, and thus $P^{(2)}_{as}$, $P^{(2)}_{bs}$, $P^{(2)}_{cs}$ and $P^{(2)}_{rs}$ are not satisfied. Furthermore, the existing primitive form is properly primitive.

Subcase (iv)$_{24122}$
$$\begin{cases} \epsilon_4 > \epsilon_1 \geq 1,\ \epsilon_4 \equiv \epsilon_3 + 1 \pmod{2},\ \epsilon_3 = \epsilon_2, \\ \epsilon_5 \equiv 0 \pmod{2},\ h_2 = 1,\ k_2 = \epsilon_4 - \epsilon_1, \\ A = 2^{\epsilon_1}A_2,\ s_1 = 2^{(\epsilon'-\epsilon_4+1)/2} s_3,\ c \equiv 0 \\ \text{or } 1 \pmod{2} \text{ according as } r_1 \text{ satisfies} \\ \Omega_3 r_1^2 + A_2 \equiv 0 \text{ or } 2^{\epsilon_4-\epsilon_1} \pmod{2^{\epsilon_4-\epsilon_1+1}}. \end{cases}$$

$\epsilon_1 + \epsilon_4 = 0$ is impossible since $\epsilon_4 > \epsilon_1$, and thus $P^{(2)}_{ab}$, $P^{(1)}_{bc}$, $P^{(1)}_{br}$ and $P^{(1)}_{bs}$ are not satisfied. If $\epsilon_1 + n_2 = 0$, then $\epsilon_1 = n_2 = 0$. But $\epsilon_1 = 0$ and $\epsilon_3 < \epsilon' = \epsilon_1 + \epsilon_2 \Rightarrow \epsilon_3 < \epsilon_2$, which is impossible since $\epsilon_3 = \epsilon_2$, and thus $P^{(2)}_{ar}$, $P^{(2)}_{br}$, $P^{(2)}_{cr}$ and $P^{(1)}_{rs}$ are not satisfied. If $n_1 = 0$, then s_1 is odd. But $s_1 = 2^{(\epsilon'-\epsilon_4+1)/2} s_3$ and s_1 odd $\Rightarrow$ s_3 odd and $\epsilon_4 = \epsilon' + 1 > \epsilon'$, which is impossible since $\epsilon_4 < \epsilon'$, and thus $P^{(2)}_{as}$, $P^{(2)}_{bs}$, $P^{(2)}_{cs}$ and $P^{(2)}_{rs}$ are not satisfied. Moreover, the existing primitive form is properly primitive.

Subcase $(\mathrm{iv})_{2422}$

$$\left\{\begin{array}{l}
\epsilon_4 > \epsilon_1 \geq 1,\ \epsilon_4 \equiv \epsilon_3 + 1 \pmod 2, \\
\epsilon_3 < \epsilon_2,\ \epsilon_1 \equiv 1 \pmod 2,\quad h_3 = \epsilon_2 - \epsilon_3, \\
k_2 = \epsilon_4 - \epsilon_1,\ A = 2^{\epsilon_1}A_2, \\
s_1 = 2^{(\epsilon_1+\epsilon_3-\epsilon_4)/2} s_3,\ s_3A_2r_1 \text{ odd}, \\
c \equiv 0 \text{ or } 1 \pmod 2 \text{ according as } r_1 \\
\text{satisfies } \Omega_3 r_1^2 + A_2 \equiv 0 \text{ or } 2^{\epsilon_4-\epsilon_1} \\
(\mathrm{mod}\ 2^{\epsilon_4-\epsilon_1+1}).
\end{array}\right.$$

$\epsilon_1 + \epsilon_4 = 0$ is impossible since $\epsilon_4 > \epsilon_1$, and thus $P_{ab}^{(2)}$, $P_{bc}^{(1)}$, $P_{br}^{(1)}$ and $P_{bs}^{(1)}$ are not satisfied. If $\epsilon_1 + n_2 = 0$, then $\epsilon_1 = n_2 = 0$. But $\epsilon_1 = 0$ is impossible since $\epsilon_1 \equiv 1 \pmod 2$, and thus $P_{ar}^{(2)}$, $P_{br}^{(2)}$, $P_{cr}^{(2)}$ and $P_{rs}^{(1)}$ are not satisfied. If $n_1 = 0$, then s_1 is odd. But $s_1 = 2^{(\epsilon_1+\epsilon_3-\epsilon_4)/2} s_3$, s_1 odd and s_3 odd $\Rightarrow \epsilon_4 = \epsilon_1 + \epsilon_3 \geq \epsilon_3$, which is impossible since $\epsilon_4 < \epsilon_3$, and thus $P_{as}^{(2)}$, $P_{bs}^{(2)}$, $P_{cs}^{(2)}$ and $P_{rs}^{(2)}$ are not satisfied. Further, the existing primitive form is properly primitive.

Subcase $(\mathrm{iv})_{243}$

$$\left\{\begin{array}{l}
\epsilon_4 > \epsilon_1,\ \epsilon_4 \equiv \epsilon_3 + 1 \pmod 2,\ \epsilon_1 = 0, \\
\epsilon_4 = 1,\ \epsilon_3 \equiv 0 \pmod 2,\quad h_3 = \epsilon_2 - \epsilon_3 - 1, \\
k_3 = 1,\ A = 2A_1,\ s_1 = 2^{\epsilon_3/2} s_2,\ r_1 = 2r_2, \\
c \equiv A_1 s_2 \equiv 1 \pmod 2 \text{ by choice of } s_2 \text{ if} \\
\epsilon_2 > \epsilon_3 + 1 \text{ and } A_1 \equiv s_2 + 1 \equiv 1 \pmod 2 \\
\text{if } \epsilon_2 = \epsilon_3 + 1.
\end{array}\right.$$

$\varepsilon_1 + \varepsilon_4 = 0$ is impossible since $\varepsilon_4 > \varepsilon_1$, and thus *$P^{(2)}_{ab}$, $P^{(1)}_{bc}$, $P^{(1)}_{br}$ and $P^{(1)}_{bs}$ are not satisfied.* If $\varepsilon_1 + n_2 = 0$, then $\varepsilon_1 = n_2 = 0$. But $n_2 = 0 \Rightarrow r_1$ is odd, which is impossible since $r_1 = 2r_2$, and thus *$P^{(2)}_{ar}$, $P^{(2)}_{br}$, $P^{(2)}_{cr}$ and $P^{(1)}_{rs}$ are not satisfied.* If $n_1 = 0$, then s_1 is odd. But $s_1 = 2^{\varepsilon_3/2} s_2$ and s_1 odd $\Rightarrow s_2$ odd and $\varepsilon_3 = 0$, which is impossible since $\varepsilon_3 = 0$ and $\varepsilon_4 < \varepsilon_3 \Rightarrow \varepsilon_4 < 0$, and thus *$P^{(2)}_{as}$, $P^{(2)}_{bs}$, $P^{(2)}_{cs}$ and $P^{(2)}_{rs}$ are not satisfied.* Furthermore, the existing primitive form is properly primitive.

Summaries of primitive (properly and improperly) forms for subcases of theorem 1 follow in which *$P^{(i)}_{uv}$: impossible* means $P^{(i)}_{uv}$ is not satisfied and there does not exist a primitive form with $(u, v) = 1$ and u or v odd according as $i = 1$ or 2, where $u, v \in \{a, b, c, r, s\}$, and u precedes v; *$P^{(i)}_{uv}$: PP* means if $P^{(i)}_{uv}$ is satisfied, then there exists a properly primitive form with $(u, v) = 1$ and u or v odd according as $i = 1$ or 2; *$P^{(i)}_{uv}$: PP iff c odd* means if $P^{(i)}_{uv}$ is satisfied, then there exists a primitive form with $(u, v) = 1$ and u or v odd according as $i = 1$ or 2 and the primitive form is properly primitive iff c is odd; in the same way *$P^{(i)}_{uv}$: PP iff a or c odd*, *$P^{(i)}_{uv}$: PP iff b or c odd* and *$P^{(i)}_{uv}$: PP iff a or b or c odd* are interpreted.

Summary of primitive (properly and improperly) forms for subcases $(i)_1$, $(i)_3$, $(i)_{52}$ and $(iii)_{211}$:

$$\left.\begin{array}{l}P^{(1)}_{ab}\\ P^{(2)}_{ab}\\ P^{(1)}_{ac}\end{array}\right\}\text{ Impossible}$$

$P^{(2)}_{ac}$: PP

$$\left.\begin{array}{l}P^{(1)}_{ar}\\ P^{(2)}_{ar}\\ P^{(1)}_{as}\end{array}\right\}\text{ Impossible}$$

$P^{(2)}_{as}$: PP iff c odd

$P^{(1)}_{bc}$: Impossible

$P^{(2)}_{bc}$: PP

$$\left.\begin{array}{l}P^{(1)}_{br}\\ P^{(2)}_{br}\\ P^{(1)}_{bs}\end{array}\right\}\text{ Impossible}$$

$P^{(2)}_{bs}$: PP iff c odd

$P^{(1)}_{cr}$: PP

$P^{(2)}_{cr}$: Impossible

$P^{(1)}_{cs}$: PP

$P^{(2)}_{cs}$: PP iff c odd

$P^{(1)}_{rs}$: Impossible

$P^{(2)}_{rs}$: PP iff c odd

Summary of primitive (properly and improperly) forms for subcase $(i)_2$:

$P^{(1)}_{ab}$: PP

$P^{(2)}_{ab}$: Impossible

$$\left.\begin{array}{l}P^{(1)}_{ac}\\ P^{(2)}_{ac}\\ P^{(1)}_{ar}\end{array}\right\}\text{ PP}$$

$P^{(2)}_{ar}$: PP iff a or c odd

$P^{(1)}_{as}$: PP

$P^{(1)}_{br}$: Impossible

$P^{(2)}_{br}$: PP iff a or c odd

$P^{(1)}_{bs}$: Impossible

$P^{(2)}_{bs}$: PP iff a or c odd

$P^{(1)}_{cr}$: PP

$P^{(2)}_{cr}$: PP iff a or c odd

$P^{(1)}_{cs}$: PP

Subcase $(i)_2$ continued

$P^{(2)}_{as}$: PP iff a or c odd

$P^{(1)}_{bc}$: Impossible

$P^{(2)}_{bc}$: PP

$$\left.\begin{array}{l} P^{(2)}_{cs} \\ P^{(1)}_{rs} \\ P^{(2)}_{rs} \end{array}\right\} \text{PP iff a or c odd}$$

Summary of primitive (properly and improperly) forms for subcase $(i)_4$:

In this subcase, if any of the 20 conditions $P^{(1)}_{ab}$, ... ,$P^{(2)}_{rs}$ are satisfied, then there exists a properly primitive form.

Summary of primitive (properly and improperly) forms for subcase $(i)_{51}$:

$P^{(1)}_{ab}$: PP

$P^{(2)}_{ab}$: Impossible

$$\left.\begin{array}{l} P^{(1)}_{ac} \\ P^{(2)}_{ac} \\ P^{(1)}_{ar} \end{array}\right\} \text{PP}$$

$P^{(2)}_{ar}$: Impossible

$P^{(1)}_{as}$: PP

$P^{(2)}_{as}$: PP iff a or c odd

$P^{(1)}_{bc}$: Impossible

$P^{(2)}_{bc}$: PP

$$\left.\begin{array}{l} P^{(1)}_{br} \\ P^{(2)}_{br} \\ P^{(1)}_{bs} \end{array}\right\} \text{Impossible}$$

$P^{(2)}_{bs}$: PP iff a or c odd

$P^{(1)}_{cr}$: PP

$P^{(2)}_{cr}$: Impossible

$P^{(1)}_{cs}$: PP

$P^{(2)}_{cs}$: PP iff a or c odd

$P^{(1)}_{rs}$: Impossible

$P^{(2)}_{rs}$: PP iff a or c odd

Summary of primitive (properly and improperly) forms for subcases $(i)_{61}$ and $(i)_{62}$:

$P^{(1)}_{ab}$: PP

$P^{(2)}_{ab}$: Impossible

$$\left.\begin{array}{l}P^{(1)}_{ac}\\ P^{(2)}_{ac}\\ P^{(1)}_{ar}\end{array}\right\}\text{ PP}$$

$P^{(2)}_{ar}$: Impossible

$$\left.\begin{array}{l}P^{(1)}_{as}\\ P^{(2)}_{as}\end{array}\right\}\text{ PP}$$

$P^{(1)}_{bc}$: Impossible

$P^{(2)}_{bc}$: PP

$$\left.\begin{array}{l}P^{(1)}_{br}\\ P^{(2)}_{br}\\ P^{(1)}_{bs}\end{array}\right\}\text{ Impossible}$$

$$\left.\begin{array}{l}P^{(2)}_{bs}\\ P^{(1)}_{cr}\end{array}\right\}\text{ PP}$$

$P^{(2)}_{cr}$: Impossible

$$\left.\begin{array}{l}P^{(1)}_{cs}\\ P^{(2)}_{cs}\end{array}\right\}\text{ PP}$$

$P^{(1)}_{rs}$: Impossible

$P^{(2)}_{rs}$: PP

Summary of primitive (properly and improperly) forms for subcase $(ii)_{13}$:

$P^{(1)}_{ab}$: Impossible

$P^{(2)}_{ab}$: PP

$P^{(1)}_{ac}$: Impossible

$P^{(2)}_{ac}$: PP

$P^{(1)}_{ar}$: Impossible

$P^{(2)}_{ar}$: PP iff b or c odd

$P^{(1)}_{as}$: Impossible

$P^{(1)}_{br}$: PP

$P^{(2)}_{br}$: PP iff b or c odd

$P^{(1)}_{bs}$: PP

$P^{(2)}_{bs}$: PP iff b or c odd

$P^{(1)}_{cr}$: PP

$P^{(2)}_{cr}$: PP iff b or c odd

$P^{(1)}_{cs}$: PP

Subcase $(ii)_{13}$ continued

$P^{(2)}_{as}$: PP iff b or c odd

$$\left.\begin{array}{l}P^{(1)}_{bc}\\ P^{(2)}_{bc}\end{array}\right\}\text{ PP}$$

$$\left.\begin{array}{l}P^{(2)}_{cs}\\ P^{(1)}_{rs}\\ P^{(2)}_{rs}\end{array}\right\}\text{ PP iff b or c odd}$$

Summary of primitive (properly and improperly) forms for subcases $(ii)_{14}$ and $(iii)_{2221}$:

$$\left.\begin{array}{l}P^{(1)}_{ab}\\ P^{(2)}_{ab}\\ P^{(1)}_{ac}\end{array}\right\}\text{ Impossible}$$

$P^{(2)}_{ac}$: PP

$P^{(1)}_{ar}$: Impossible

$P^{(2)}_{ar}$: PP iff c odd

$P^{(1)}_{as}$: Impossible

$P^{(2)}_{as}$: PP iff c odd

$P^{(1)}_{bc}$: Impossible

$P^{(2)}_{bc}$: PP

$P^{(1)}_{br}$: Impossible

$P^{(2)}_{br}$: PP iff c odd

$P^{(1)}_{bs}$: Impossible

$P^{(2)}_{bs}$: PP iff c odd

$P^{(1)}_{cr}$: PP

$P^{(2)}_{cr}$: PP iff c odd

$P^{(1)}_{cs}$: PP

$$\left.\begin{array}{l}P^{(2)}_{cs}\\ P^{(1)}_{rs}\\ P^{(2)}_{rs}\end{array}\right\}\text{ PP iff c odd}$$

Summary of primitive (properly and improperly) forms for subcases $(ii)_{23}$ and $(iv)_{1321}$:

$P^{(1)}_{ab}$: Impossible

$P^{(2)}_{ab}$: PP

$P^{(1)}_{ac}$: Impossible

$P^{(1)}_{br}$: PP

$P^{(2)}_{br}$: PP iff b or c odd

$P^{(1)}_{bs}$: PP

Subcases $(ii)_{23}$ and $(iv)_{1321}$ continued

$P^{(2)}_{ac}$: PP

$P^{(1)}_{ar}$: Impossible

$P^{(2)}_{ar}$: PP iff b or c odd

$$\left.\begin{array}{l} P^{(1)}_{as} \\ P^{(2)}_{as} \end{array}\right\} \text{Impossible}$$

$$\left.\begin{array}{l} P^{(1)}_{bc} \\ P^{(2)}_{bc} \end{array}\right\} \text{PP}$$

$P^{(2)}_{bs}$: Impossible

$P^{(1)}_{cr}$: PP

$P^{(2)}_{cr}$: PP iff b or c odd

$P^{(1)}_{cs}$: PP

$P^{(2)}_{cs}$: Impossible

$P^{(1)}_{rs}$: PP iff b or c odd

$P^{(2)}_{rs}$: Impossible

Summary of primitive (properly and improperly) forms for subcases $(ii)_{24}$ and $(iv)_{2321}$:

$$\left.\begin{array}{l} P^{(1)}_{ab} \\ P^{(2)}_{ab} \\ P^{(1)}_{ac} \end{array}\right\} \text{Impossible}$$

$P^{(2)}_{ac}$: PP

$P^{(1)}_{ar}$: Impossible

$P^{(2)}_{ar}$: PP iff c odd

$$\left.\begin{array}{l} P^{(1)}_{as} \\ P^{(2)}_{as} \\ P^{(1)}_{bc} \end{array}\right\} \text{Impossible}$$

$P^{(2)}_{bc}$: PP

$P^{(1)}_{br}$: Impossible

$P^{(2)}_{br}$: PP iff c odd

$$\left.\begin{array}{l} P^{(1)}_{bs} \\ P^{(2)}_{bs} \end{array}\right\} \text{Impossible}$$

$P^{(1)}_{cr}$: PP

$P^{(2)}_{cr}$: PP iff c odd

$P^{(1)}_{cs}$: PP

$P^{(2)}_{cs}$: Impossible

$P^{(1)}_{rs}$: PP iff c odd

$P^{(2)}_{rs}$: Impossible

Summary of primitive (properly and improperly) forms for subcase $(\mathrm{iii})_{111}$:

$$\left.\begin{array}{l} P^{(1)}_{ab}\\ P^{(2)}_{ab}\\ P^{(1)}_{ac}\\ P^{(2)}_{ac}\\ P^{(1)}_{ar} \end{array}\right\}\ \text{PP}$$

$P^{(2)}_{ar}$: PP iff a or b or c odd

$P^{(1)}_{as}$: PP

$P^{(2)}_{as}$: PP iff a or b or c odd

$$\left.\begin{array}{l} P^{(1)}_{bc}\\ P^{(2)}_{bc} \end{array}\right\}\ \text{PP}$$

$P^{(1)}_{br}$: PP

$P^{(2)}_{br}$: PP iff a or b or c odd

$P^{(1)}_{bs}$: PP

$P^{(2)}_{bs}$: PP iff a or b or c odd

$P^{(1)}_{cr}$: PP

$P^{(2)}_{cr}$: PP iff a or b or c odd

$P^{(1)}_{cs}$: PP

$$\left.\begin{array}{l} P^{(2)}_{cs}\\ P^{(1)}_{rs}\\ P^{(2)}_{rs} \end{array}\right\}\ \text{PP iff a or b or c odd}$$

Summary of primitive (properly and improperly) forms for subcases $(\mathrm{iii})_{112}$, $(\mathrm{iii})_{121}$, $(\mathrm{iii})_{2211}$, $(\mathrm{iii})_{2222}$, $(\mathrm{iv})_{1311}$, $(\mathrm{iv})_{1312}$, $(\mathrm{iv})_{13221}$, $(\mathrm{iv})_{1411}$, $(\mathrm{iv})_{1412}$, $(\mathrm{iv})_{1421}$, $(\mathrm{iv})_{14221}$, $(\mathrm{iv})_{2311}$, $(\mathrm{iv})_{2312}$, $(\mathrm{iv})_{2411}$, $(\mathrm{iv})_{24122}$, $(\mathrm{iv})_{2422}$ and $(\mathrm{iv})_{243}$:

$$\left.\begin{array}{l} P^{(1)}_{ab}\\ P^{(2)}_{ab}\\ P^{(1)}_{ac} \end{array}\right\}\ \text{Impossible}$$

$P^{(2)}_{ac}$: PP

$$\left.\begin{array}{l} P^{(1)}_{br}\\ P^{(2)}_{br}\\ P^{(1)}_{bs}\\ P^{(2)}_{bs} \end{array}\right\}\ \text{Impossible}$$

Subcases $(iii)_{112}, \ldots, (iv)_{243}$ continued

$$\left.\begin{array}{l} P_{ar}^{(1)} \\ P_{ar}^{(2)} \\ P_{as}^{(1)} \\ P_{as}^{(2)} \\ P_{bc}^{(1)} \end{array}\right\} \text{Impossible} \qquad \begin{array}{l} P_{cr}^{(1)}: \text{PP} \\ P_{cr}^{(2)}: \text{Impossible} \\ P_{cs}^{(1)}: \text{PP} \end{array}$$

$$P_{bc}^{(2)}: \text{PP} \qquad \left.\begin{array}{l} P_{cs}^{(2)} \\ P_{rs}^{(1)} \\ P_{rs}^{(2)} \end{array}\right\} \text{Impossible}$$

Summary of primitive (properly and improperly) forms for subcases $(iv)_{13222}$ and $(iv)_{14222}$:

In these subcases, none of the 20 conditions $P_{ab}^{(1)}$, $\ldots, P_{rs}^{(2)}$ is satisfied, and thus there does not exist a primitive form.

Some examples of primitive (properly and improperly) forms:

Example 3.1 (a): [For subcase $(i)_1$]

$$\begin{cases} \varepsilon_3 \le \varepsilon' \le \varepsilon_4,\ \varepsilon_2 < \varepsilon_3,\ \varepsilon_1 < \varepsilon_4 = \varepsilon',\ h_1 = \varepsilon_3 - \varepsilon_2, \\ k_2 = \varepsilon_4 - \varepsilon_1,\ A = 2^{\varepsilon_1} A_2,\ s_1 A_2 r_1 \text{ odd},\ c \equiv 0 \text{ or } 1 \pmod 2 \\ \text{according as } r_1 \text{ satisfies } \Omega_3 r_1^2 + A_2 \equiv 0 \text{ or } 2^{\varepsilon_4 - \varepsilon_1} \\ (\text{mod } 2^{\varepsilon_4 - \varepsilon_1 + 1}). \end{cases}$$

Let $\varepsilon_1 = 1$, $\varepsilon_2 = 4$, $\varepsilon_3 = 5$, $\varepsilon_4 = 5$, $\Omega_1 = 3$, $\Delta_1 = 5$, $a_1 = 7$ and $b_2 = q$ an odd prime. By (1.2), $\delta_1 = 15$, $D = 1$, $a_2 = 7$,

$\delta_2 = 15$, $\Omega_2 = 1$, $\Omega_3 = 3$ and $D_1 = D_2 = 1$. Since $h_1 = 1$ and $k_2 = 4$, I and I_1 of (1.5) are applicable here, and thus $k' = 3$. Now $\gamma \equiv 2\cdot7\cdot3\cdot7 - 15 \equiv -1 \pmod{8}$. Take $\gamma = -1$. Now $b_2D_2\gamma \equiv -q \equiv 1 \pmod{2^4}$, and thus $q \equiv -1 \pmod{16}$. By (1.4), $(q|7) = (-15|7) = -1$ since $h = h_2 + h_3 = 0$ and $(q|15\cdot3\cdot7) = (-1)^{(q-1)/2\cdot(15\cdot3\cdot7+1)/2}(2|q) = (2|q)$ $= (-1)^{(q^2-1)/8}$ since $k = h_1 + h_3 + k_1 + k_3 = 1$. Thus $q \equiv -1 \pmod{16}$, $(q|7) = -1$ and $(q|5) = (-1)^{(q^2+7)/8}$. Take $q = 47$. By (1.7) and (1.9), $47s_1^2 \equiv -15 \pmod{14}$, and thus $s_1 \equiv \pm 5 \pmod{14}$. Take $s_1 = 5$. Then $A_2 = 85$ by $(1.6)_1$. By (1.8) and (1.10), $3r_1^2 \equiv -85 \pmod{2^4\cdot47}$, and thus $r_1 \equiv \pm 35(2^4\cdot47)$. Take $r_1 = 35$. By $(1.6)_2$ and (1.11), $c = 5$. By (1.1), $\Omega = 2\cdot3$, $\Delta = 2^4\cdot5$, $a = 2^5\cdot7$ and $b = 2^6\cdot3\cdot47$. By (1.12), $s = D_1D_2s_1 = 5$. By (1.13), $r = 2^{\varepsilon_1}\Omega_2\Omega_3r_1 = 2\cdot3\cdot5\cdot7$.

$$d = \begin{vmatrix} 2^5\cdot7 & 0 & 5 \\ 0 & 2^6\cdot3\cdot47 & 2\cdot3\cdot5\cdot7 \\ 5 & 2\cdot3\cdot5\cdot7 & 5 \end{vmatrix} = 2^6\cdot3^2\cdot5 = \Omega^2\Delta.$$

Since $(a, b, c, r, s) = 1$ and (a, b, c) is odd, the form of this example is properly primitive. Further note from

(3.1) - (3.3) that $n_1 = 0$, $s_1' = 5$; $n_2 = 0$, $r_1' = 35$; $n_3 = 0$, $c' = 5$. Now from the summary of primitive (properly and improperly) forms for subcase $(i)_1$, observe the following:

$P_{ab}^{(1)}$, $P_{ac}^{(1)}$, $P_{ar}^{(1)}$ and $P_{as}^{(1)}$ are not satisfied since a is even, and thus the form of this example is not primitive with (a, bcrs) = 1 and a odd holding simultaneously. $P_{ab}^{(2)}$, $P_{bc}^{(1)}$, $P_{br}^{(1)}$ and $P_{bs}^{(1)}$ are not satisfied since b is even, and thus the form of this example is not primitive with (b, acrs) = 1 and b odd. $P_{ar}^{(2)}$, $P_{br}^{(2)}$, $P_{cr}^{(2)}$ and $P_{rs}^{(1)}$ are not satisfied since r is even, and thus the form of this example is not primitive with (r, abcs) = 1 and r odd. $P_{ac}^{(2)}$ is satisfied as $n_3 = 0$ and $(a_1, c') = 1$, and thus the form of this example is properly primitive with (a, c) = 1 and c odd. $P_{as}^{(2)}$ is satisfied as $n_1 = 0$ and D = 1, and thus the form of this example is primitive with (a, s) = 1 and s odd. $P_{bc}^{(2)}$ is satisfied as $n_3 = 0$ and $(\Omega_1 b_2, c') = 1$, and thus the form of this example is properly primitive with (b, c) = 1 and c odd. $P_{bs}^{(2)}$ is satisfied as $n_1 = 0$ and $(\Omega_1, Ds_1') = (b_2, s_1') = 1$, and thus the form of this example is primitive with (b, s) = 1 and s odd. $P_{cr}^{(1)}$ is not satisfied since $(c', \Omega_1 r_1') > 1$, and thus the form of this example is not primitive with (c, r) = 1 and c odd. $P_{cs}^{(1)}$ and $P_{cs}^{(2)}$ are not satisfied since $(c', Ds_1') > 1$, and thus the form of this example is not primitive with $(c, s) = 1$. Finally $P_{rs}^{(2)}$ is not satisfied since $(\Omega_1 r_1', Ds_1') > 1$, and thus the form of this example is not primitive with $(r, s) = 1$ and s odd.

Example 3.1 (b): [For subcase $(i)_1$]

Using the data of example 3.1 (a), we have $\epsilon_1 = 1$, $\epsilon_2 = 4$, $\epsilon_3 = 5$, $\epsilon_4 = 5$, $\Omega_1 = 3$, $\Delta_1 = 5$, $a_1 = 7$, $b_2 = q = 47$, $h_1 = 1$, $k_2 = 4$, $\delta_1 = 15$, $D = 1$, $a_2 = 7$, $\delta_2 = 15$, $\Omega_2 = 1$, $\Omega_3 = 3$ and $D_1 = D_2 = 1$. Now by theorem 2, an infinite number of values for each of s_1, r_1 and c can be determined as follows:

By (2.6), $\alpha \equiv 3 \pmod{14}$. Choose $\alpha = 3$. By (2.10), $q_1 = 10$. In example 3.1 (a), $s_1 \equiv \pm 5 \pmod{14}$, and thus by (2.13), $\lambda = 5$. By (2.11), $q_2 = 5$. In example 3.1 (a), $r_1 \equiv \pm 35 \pmod{2^4 \cdot 47}$, and thus by (2.20), $\mu = 35$. By (1.11) and (2.3), $c = c(\beta, \rho) = 7\beta^2/8 + 2^4 \cdot 3 \cdot 47\rho^2 \pm 5\beta/8$ $\pm 2 \cdot 3 \cdot 35\rho + 5$, where ρ is arbitrary and by (2.4), β is to be chosen such that $\beta(7\beta \pm 5) \equiv 0 \pmod 8$ since $h_2 < k_2$, and thus $\beta \equiv 0, 3$ or $5 \pmod 8$. By (1.9) and (2.1), $s_1 = 14\beta \pm 5$. By (1.10) and (2.2), $r_1 = 2^4 \cdot 47\rho \pm 35$.

Observe that $\beta = 0$ and $\rho = 0$ yield $s_1 = 5$, $r_1 = 35$ and $c = 5$, which were obtained in example 3.1 (a). Recall that the signs in the expressions for s_1 and r_1 agree with those of the coefficients of β and ρ respectively in the expression for c. Now choose $\beta = 3$ and $\rho = 0$. Take the minus sign in the expression for s_1 since $\beta \equiv 3 \pmod 8$ is the solution of $7\beta - 5 \equiv 0 \pmod 8$ and obtain $s_1 = 37$, $r_1 = 35$ and $c = 11$. By choosing other values for β and ρ, different sets of values of s_1, r_1 and c are similarly determined. By (1.12), $s = D_1D_2s_1 = 37$. By (1.13), $r = 2^{\varepsilon_1}\Omega_2\Omega_3r_1 = 2\cdot3\cdot5\cdot7$.

$$d = \begin{vmatrix} 2^5\cdot7 & 0 & 37 \\ 0 & 2^6\cdot3\cdot47 & 2\cdot3\cdot5\cdot7 \\ 37 & 2\cdot3\cdot5\cdot7 & 11 \end{vmatrix} = 2^6\cdot3^2\cdot5 = \Omega^2\Delta.$$

Since (a, b, c, r, s) = 1 and (a, b, c) is odd, the form of this example is properly primitive. Further note from (3.1) - (3.3) that $n_1 = 0$, $s_1' = 37$; $n_2 = 0$, $r_1' = 35$; $n_3 = 0$, $c' = 11$. Now from the summary of primitive (properly and improperly) forms for subcase $(i)_1$, observe the following:

$P_{ab}^{(1)}$, $P_{ac}^{(1)}$, $P_{ar}^{(1)}$ and $P_{as}^{(1)}$ are not satisfied since a is even, and thus the form of this example is not primitive with (a, bcrs) = 1 and a odd. $P_{ab}^{(2)}$, $P_{bc}^{(1)}$, $P_{br}^{(1)}$ and $P_{bs}^{(1)}$ are not satisfied since b is even, and thus the form of this example is not primitive with (b, acrs) = 1 and b odd. $P^{(2)}_{ar}$, $P^{(2)}_{br}$, $P^{(2)}_{cr}$ and $P^{(1)}_{rs}$ are not satisfied since r is even, and thus the form of this example is not primitive with (r, abcs) = 1 and r odd. $P^{(2)}_{ac}$ is satisfied as $n_3 = 0$ and $(a_1, c') = 1$, and thus the form of this example is properly primitive with (a, c) = 1 and c odd. $P^{(2)}_{as}$ is satisfied as $n_1 = 0$ and D = 1, and thus the form of this example is primitive with (a, s) = 1 and s odd. $P^{(2)}_{bc}$ is satisfied as $n_3 = 0$ and $(\Omega_1 b_2, c') = 1$, and thus the form of this example is properly primitive with (b, c) = 1 and c odd. $P^{(2)}_{bs}$ is satisfied as $n_1 = 0$ and $(\Omega_1, Ds_1') = (b_2, s_1') = 1$, and thus the form of this example is primitive with (b, s) = 1 and s odd. $P^{(1)}_{cr}$ is satisfied as $n_3 = 0$ and $(c', \Omega_1 r_1') = 1$, and thus the form of this example is properly primitive with (c, r) = 1 and c odd. $P^{(1)}_{cs}$ is satisfied as $n_3 = 0$ and $(c', Ds_1') = 1$, and thus the form of this example is properly primitive with (c, s) = 1 and c odd. $P^{(2)}_{cs}$ is satisfied since $n_1 = 0$ and $(c', Ds_1') = 1$, and thus the form of this example is primitive with (c, s) = 1 and s odd. Finally $P^{(2)}_{rs}$ is satisfied as $n_1 = 0$ and $(\Omega_1 r_1', Ds_1') = 1$, and thus the form of this example is primitive with (r, s) = 1 and s odd.

Example 3.2: [For subcase $(ii)_{14}$]

$$\left\{\begin{array}{l} \epsilon_4 \le \epsilon' \le \epsilon_3,\ \epsilon_4 \ne \epsilon_3,\ s_1 = 2^{[(\epsilon'-\epsilon_4+1)/2]} s_2,\ \epsilon_4 > \epsilon_1, \\ \epsilon_4 \equiv \epsilon' \pmod{2},\ h_1 = \epsilon_3 - \epsilon_2,\ k_2 = \epsilon_4 - \epsilon_1,\ A = 2^{\epsilon_1} A_1, \\ s_2 A_1 r_1 \text{ odd if } \epsilon_2 < \epsilon_3;\ A_1 r_1 \equiv s_2 + 1 \equiv 1 \pmod{2} \text{ or} \\ (A_1/4)(r_1/2)s_2 \equiv 1 \pmod{2} \text{ if } \epsilon_2 = \epsilon_3;\ c \equiv 0 \text{ or } 1 \pmod{2} \\ \text{according as } r_1 \text{ satisfies } \Omega_3 r_1^2 + A_1 \equiv 0 \text{ or } 2^{\epsilon_4-\epsilon_1} \\ (\text{mod } 2^{\epsilon_4-\epsilon_1+1}). \end{array}\right.$$

Let $\epsilon_1 = 1$, $\epsilon_2 = 1$, $\epsilon_3 = 3$, $\epsilon_4 = 2$, $\Omega_1 = 3$, $\Delta_1 = 5$, $a_1 = 7$ and $b_2 = q$ an odd prime. By (1.2), $\delta_1 = 15$, $D = 1$, $a_2 = 7$, $\delta_2 = 15$, $\Omega_2 = 1$, $\Omega_3 = 3$ and $D_1 = D_2 = 1$. Since $h_1 = 2$, (1.5) is applicable, and thus $\alpha \equiv 3\cdot 15 \equiv 1 \pmod{4}$. Take $\alpha = 1$. Now $b_2 D_2 \alpha \equiv b_2 \equiv q \equiv 1 \pmod{4}$, and thus $q \equiv 1 \pmod{4}$. From (1.4), $(q|7) = (-15|7) = -1$ since $h = h_2 + h_3 = 0$ and $(q|15\cdot 3\cdot 7) = (-1)^{(q-1)/2\cdot(15\cdot 3\cdot 7+1)/2}(2^2|q) = 1$ since $k = h_1 + h_3 + k_1 + k_3 = 2$. Thus $q \equiv 1 \pmod{4}$, $(q|7) = -1$ and $(q|5) = -1$. Take $q = 13$. By (1.7) and (1.9), $13 s_2^2 \equiv -15$ (mod 28), and thus $s_2 \equiv \pm 1 \pmod{28}$. Take $s_2 = 1$. Now $s_1 = 2^{[(\epsilon'-\epsilon_4+1)/2]} s_2 = s_2 = 1$. By $(1.6)_1$, $A_1 = 1$. By (1.8) and (1.10), $3r_1^2 \equiv -1 \pmod{26}$, and thus $r_1 \equiv \pm 11$ (mod 26). Take $r_1 = 11$. By $(1.6)_2$ and (1.11), $c = 14$. By (1.1), $\Omega = 2\cdot 3$, $\Delta = 2\cdot 5$, $a = 2^3\cdot 7$ and $b = 2^3\cdot 3\cdot 13$. By

(1.12), $s = D_1D_2s_1 = 1$. By (1.13), $r = 2^{\varepsilon_1}\Omega_2\Omega_3r_1 = 2\cdot3\cdot11$.

$$d = \begin{vmatrix} 2^3\cdot7 & 0 & 1 \\ 0 & 2^3\cdot3\cdot13 & 2\cdot3\cdot11 \\ 1 & 2\cdot3\cdot11 & 14 \end{vmatrix} = 2^3\cdot3^2\cdot5 = \Omega^2\Delta.$$

Since $(a, b, c, r, s) = 1$ and (a, b, c) is even, the form of this example is improperly primitive. Further note from (3.1) - (3.3) that $n_1 = 0$, $s_1' = 1$; $n_2 = 0$, $r_1' = 11$; $n_3 = 1$, $c' = 7$. Now from the summary of primitive (properly and improperly) forms for subcase $(ii)_{14}$, observe the following:

$P_{ab}^{(1)}$, $P_{ac}^{(1)}$, $P_{ar}^{(1)}$ and $P_{as}^{(1)}$ are not satisfied since a is even, and thus the form of this example is not primitive with $(a, bcrs) = 1$ and a odd. $P_{ab}^{(2)}$, $P_{bc}^{(1)}$, $P_{br}^{(1)}$ and $P_{bs}^{(1)}$ are not satisfied since b is even, and thus the form of this example is not primitive with $(b, acrs) = 1$ and b odd. $P_{ac}^{(2)}$, $P_{bc}^{(2)}$, $P_{cr}^{(1)}$ and $P_{cs}^{(1)}$ are not satisfied since c is even, and thus the form of this example is not primitive with $(c, abrs) = 1$ and c odd. $P_{ar}^{(2)}$, $P_{br}^{(2)}$, $P_{cr}^{(2)}$ and $P_{rs}^{(1)}$ are not satisfied since r is even, and thus the form of this example is not primitive with $(r, abcs) = 1$ and r odd. $P_{as}^{(2)}$ is satisfied as $n_1 = 0$ and $D = 1$, and thus the form of this example is primitive with $(a, s) = 1$ and s odd. $P_{bs}^{(2)}$ is satisfied as $n_1 = 0$ and $(\Omega_1, Ds_1') = (b_2, s_1') = 1$, and thus the form of this example is primitive with $(b, s) = 1$ and s odd. $P_{cs}^{(2)}$ is satisfied as $n_1 = 0$ and $(c', Ds_1') = 1$, and thus the form of this example is primitive with $(c, s) = 1$ and s odd. Finally $P_{rs}^{(2)}$ is satisfied as $n_1 = 0$ and $(\Omega_1 r_1', Ds_1') = 1$, and thus the form of this example is primitive with $(r, s) = 1$ and s odd.

Example 3.3: [For subcase $(iii)_{211}$]

$$\begin{cases} \epsilon_3 \le \epsilon_4 < \epsilon', \ \epsilon_1 < \epsilon_4 - \epsilon_3 < \epsilon_4, \ \epsilon_4 \equiv \epsilon_1 + \epsilon_3 \pmod 2, \\ h_3 = \epsilon' - \epsilon_4, \ k_2 = \epsilon_3, \ A = 2^{\epsilon_4-\epsilon_3}A_1, \ r_1 = 2^{(\epsilon_4-\epsilon_1-\epsilon_3)/2} r_2, \\ A_1 \equiv s_1 \pmod 2; \text{ if } \epsilon_3 \ge 1, \text{ then } A_1 \equiv s_1 \equiv 1 \pmod 2; \\ c \equiv 0 \text{ or } 1 \pmod 2 \text{ according as } r_2 \text{ satisfies} \\ \Omega_3 r_2^2 + A_1 \equiv 0 \text{ or } 2^{\epsilon_3} \pmod{2^{\epsilon_3+1}}. \end{cases}$$

Let $\epsilon_1 = 0$, $\epsilon_2 = 5$, $\epsilon_3 = 2$, $\epsilon_4 = 4$, $\Omega_1 = 3$, $\Delta_1 = 5$, $a_1 = 7$ and $b_2 = q$ an odd prime. By (1.2), $\delta_1 = 15$, $D = 1$, $a_2 = 7$, $\delta_2 = 15$, $\Omega_2 = 1$, $\Omega_3 = 3$ and $D_1 = D_2 = 1$. Since $h_3 = 1$ and $k_2 = 2$, I and I_3 of (1.5) are applicable, and thus $k' = 2$. Now $b_2 \equiv q \equiv 7 \cdot 3 \cdot 7 - 2 \cdot 15 \equiv 1 \pmod 4$. By (1.4), $(q|7) = (-30|7) = -1$ since $h = h_2 + h_3 = 0$ and $(q|15 \cdot 3 \cdot 7) = (-1)^{(q-1)/2 \cdot (15 \cdot 3 \cdot 7 + 1)/2}(2|q) = (2|q)$

$= (-1)^{(q^2-1)/8}$ since $k = h_1 + h_3 + k_1 + k_3 = 1$. Thus $q \equiv 1 \pmod 4$, $(q|7) = -1$ and $(q|5) = (-1)^{(q^2+7)/8}$. Choose $q = 17$. By (1.7) and (1.9), $17s_1^2 \equiv -30 \pmod 7$, and thus $s_1 \equiv \pm 2 \pmod 7$. Take $s_1 = 9$. By $(1.6)_1$, $A_1 = 201$. By (1.8) and (1.10), $3r_2^2 \equiv -201 \pmod{68}$, and thus $r_2 \equiv \pm 1 \pmod{68}$. Take $r_2 = 1$. Now $r_1 = 2^{(\varepsilon_4-\varepsilon_1-\varepsilon_3)/2} r_2 = 2r_2 = 2$. By $(1.6)_2$ and (1.11), $c = 3$. By (1.1), $\Omega = 3$, $\Delta = 2^5\cdot 5$, $a = 2^2\cdot 7$ and $b = 2^4\cdot 3\cdot 17$. By (1.12), $s = D_1D_2s_1 = 3^2$. By (1.13), $r = 2^{\varepsilon_1}\Omega_2\Omega_3r_1 = 2\cdot 3$

$$d = \begin{vmatrix} 2^2\cdot 7 & 0 & 3^2 \\ 0 & 2^4\cdot 3\cdot 17 & 2\cdot 3 \\ 3^2 & 2\cdot 3 & 3 \end{vmatrix} = 2^5\cdot 3^2\cdot 5 = \Omega^2\Delta.$$

Since $(a, b, c, r, s) = 1$ and (a, b, c) is odd, the form of this example is properly primitive. Further observe from (3.1) - (3.3) that $n_1 = 0$, $s_1' = 9$; $n_2 = 1$, $r_1' = 1$; $n_3 = 0$, $c' = 3$. Now from the summary of primitive (properly and improperly) forms for subcase $(iii)_{211}$, observe the following:

$P_{ab}^{(1)}$, $P_{ac}^{(1)}$, $P_{ar}^{(1)}$ and $P_{as}^{(1)}$ are not satisfied since a is even, and thus the form of this example is not primitive with $(a, bcrs) = 1$ and a odd. $P_{ab}^{(2)}$, $P_{bc}^{(1)}$, $P_{br}^{(1)}$ and $P_{bs}^{(1)}$ are not satisfied since b is even, and thus the form of this example is not primitive with (b, acrs) = 1 and b odd. $P_{ar}^{(2)}$, $P_{br}^{(2)}$, $P_{cr}^{(2)}$ and $P_{rs}^{(1)}$ are not satisfied since r is even, and thus the form of this example is not primitive with (r, abcs) = 1 and r odd. $P_{ac}^{(2)}$ is satisfied as $n_3 = 0$ and $(a_1, c') = 1$, and thus the form of this example is properly primitive with (a, c) = 1 and c odd. $P_{as}^{(2)}$ is satisfied as $n_1 = 0$ and D = 1, and thus the form of this example is primitive with (a, s) = 1 and s odd. $P_{bc}^{(2)}$ is not satisfied since $(\Omega_1 b_2, c') > 1$, and thus the form of this example is not primitive with (b, c) = 1 and c odd. $P_{bs}^{(2)}$ is not satisfied since $(\Omega_1, Ds_1') > 1$, and thus the form of this example is not primitive with (b, s) = 1 and s odd. $P_{cr}^{(1)}$ is not satisfied since $(c', \Omega_1 r_1') > 1$, and thus the form of this example is not primitive with (c, r) = 1 and c odd. $P_{cs}^{(1)}$ and $P_{cs}^{(2)}$ are not satisfied since $(c', Ds_1') > 1$, and thus the form of this example is not primitive with (c, s) = 1. Finally $P_{rs}^{(2)}$ is not satisfied since $(\Omega_1 r_1', Ds_1') > 1$, and thus the form of this example is not primitive with (r, s) = 1 and s odd.

Example 3.4: [For subcase $(iv)_{2311}$]

$$\begin{cases} \epsilon_4 < \epsilon_3 < \epsilon', \ \epsilon_4 > \epsilon_1, \ \epsilon_4 \equiv \epsilon_3 \pmod 2, \ \epsilon_3 \geq \epsilon_2, \\ \epsilon_5 \equiv 0 \pmod 2, \ h_1 = \epsilon_3 - \epsilon_2, \ k_2 = \epsilon_4 - \epsilon_1, \ A = 2^{\epsilon_1}A_1, \\ s_1 = 2^{(\epsilon'-\epsilon_4)/2} s_3, \ s_3A_1r_1 \text{ odd if } \epsilon_3 > \epsilon_2; \ A_1r_1 \equiv s_3 + 1 \\ \equiv 1 \pmod 2 \text{ or } (A_1/4)(r_1/2)s_3 \equiv 1 \pmod 2 \text{ if } \epsilon_3 = \epsilon_2; \\ c \equiv 0 \text{ or } 1 \pmod 2 \text{ according as } r_1 \text{ satisfies} \\ \Omega_3 r_1^2 + A_1 \equiv 0 \text{ or } 2^{\epsilon_4-\epsilon_1} \pmod{2^{\epsilon_4-\epsilon_1+1}}. \end{cases}$$

Let $\epsilon_1 = 2$, $\epsilon_2 = 8$, $\epsilon_3 = 8$, $\epsilon_4 = 6$, $\Omega_1 = 5$, $\Delta_1 = 7$, $a_1 = 3$ and $b_2 = q$ an odd prime. By (1.2), $\delta_1 = 35$, $D = 1$, $a_2 = 3$, $\delta_2 = 35$, $\Omega_2 = 1$, $\Omega_3 = 5$ and $D_1 = D_2 = 1$. Since $h_1 = h_2 = h_3 = 0$ and $k_2 = 4$, I, I_2 and I_{22} of (1.5) are applicable, and thus $k' = 3$. Now $\gamma \equiv 4 - 35 \equiv 1 \pmod 8$. Choose $\gamma = 1$. Now $b_2D_2\gamma \equiv q \equiv 1 \pmod{32}$. By (1.4), $(q|3) = (-35|3) = 1$ since $h = h_2 + h_3 = 0$ and $(q|35\cdot5\cdot3)$ $= (-1)^{(q-1)/2\cdot(35\cdot5\cdot3+1)/2} = 1$ since $k = h_1 + h_3 + k_1 + k_3$ $= 0$ and $q \equiv 1 \pmod{32}$. Thus $q \equiv 1 \pmod{32}$ and $(q|3) = (q|7) = 1$. Choose $q = 193$. By (1.7) and (1.9), $193s_3^2 \equiv -35 \pmod 3$, and thus $s_3 \equiv \pm 1 \pmod 3$. Choose $s_3 = 1$, which satisfies the condition I_{22}: $2^{h_2}s_3 \equiv 1 \pmod 2$ of (1.5). Now $s_1 = 2^{(\epsilon'-\epsilon_4)/2}s_3 = 2^2$. By $(1.6)_1$, $A_1 = 76 \equiv 0 \pmod 4$. By (1.8) and (1.10), $5r_1^2 \equiv -76 \pmod{16\cdot193}$.

Since $\epsilon_3 = \epsilon_2$, $s_3 \equiv 1 \pmod 2$ and $(A_1/4) \equiv 1 \pmod 2$, we have $(r_1/2) \equiv 1 \pmod 2$, that is, $r_1 = 2r'$, r' odd, and thus $5r'^2 \equiv -19 \pmod{4\cdot 193}$. Then $r'^2 \equiv 1 \pmod 4$ and $r'^2 \equiv 112 \pmod{193}$, that is, $r' \equiv \pm 1 \pmod 4$ and $r' \equiv \pm 43 \pmod{193}$. Choose $r' = 43$. Thus $r_1 = 2\cdot 43$. By $(1.6)_2$ and (1.11), $c = 2^2\cdot 3$. By (1.1), $\Omega = 2^2\cdot 5$, $\Delta = 2^8\cdot 7$, $a = 2^8\cdot 3$ and $b = 2^8\cdot 5\cdot 193$. By (1.12), $s = D_1D_2s_1 = 2^2$. By (1.13), $r = 2^{\epsilon_1}\Omega_2\Omega_3 r_1 = 2^3\cdot 5\cdot 43$.

$$d = \begin{vmatrix} 2^8\cdot 3 & 0 & 2^2 \\ 0 & 2^8\cdot 5\cdot 193 & 2^3\cdot 5\cdot 43 \\ 2^2 & 2^3\cdot 5\cdot 43 & 2^2\cdot 3 \end{vmatrix} = 2^{12}\cdot 5^2\cdot 7 = \Omega^2\Delta.$$

Since $(a, b, c, r, s) > 1$, the form of this example is not primitive. Further observe from (3.1) - (3.3) that $n_1 = 2$, $s_1' = 1$; $n_2 = 1$, $r_1' = 43$; $n_3 = 2$, $c' = 3$. Now from the summary of primitive (properly and improperly) forms for subcase $(iv)_{2311}$, observe the following:

$P_{ab}^{(1)}$, $P_{ac}^{(1)}$, $P_{ar}^{(1)}$ and $P_{as}^{(1)}$ are not satisfied since a is even, and thus the form of this example is not primitive with $(a, bcrs) = 1$ and a odd. $P_{ab}^{(2)}$, $P_{bc}^{(1)}$, $P_{br}^{(1)}$ and $P_{bs}^{(1)}$ are not satisfied since b is even, and thus the form of this example is not primitive with (b, acrs) = 1 and b odd. $P_{ar}^{(2)}$, $P_{br}^{(2)}$, $P_{cr}^{(2)}$ and $P_{rs}^{(1)}$ are not satisfied since r is even, and thus the form of this example is not primitive with (r, abcs) = 1 and r odd. $P_{as}^{(2)}$, $P_{bs}^{(2)}$, $P_{cs}^{(2)}$ and $P_{rs}^{(2)}$ are not satisfied since s is even, and thus the form of this example is not primitive with (s, abcr) = 1 and s odd. Finally $P_{ac}^{(2)}$, $P_{bc}^{(2)}$, $P_{cr}^{(1)}$ and $P_{cs}^{(1)}$ are not satisfied since c is even, and thus the form of this example is not primitive with (c, abrs) = 1 and c odd. Since none of the 20 conditions $P_{uv}^{(i)}$, where u, v ∈ {a, b, c, r, s}, u precedes v and i = 1, 2 is satisfied, the form of this example is not primitive,

Example 3.5: [For subcase $(i)_2$]

$$\begin{cases} \epsilon_3 \le \epsilon' \le \epsilon_4,\ \epsilon_2 = \epsilon_3,\ \epsilon_1 < \epsilon_4,\ h_2 = \epsilon_4 - \epsilon',\ k_2 = \epsilon_4 - \epsilon_1, \\ A = 2^{\epsilon_5}A_1,\ A_1 r_1 \text{ odd if } \epsilon_4 > \epsilon';\ \text{if } \epsilon_4 = \epsilon', \text{ then} \\ A_1 r_1 \equiv s_1 + 1 \equiv 1 \pmod 2 \text{ or } (A_1/4)(r_1/2)s_1 \equiv 1 \pmod 2; \\ c \equiv 0 \text{ or } 1 \pmod 2 \text{ according as } r_1 \text{ satisfies} \\ \Omega_3 r_1^2 + A_1 \equiv 0 \text{ or } 2^{\epsilon_4 - \epsilon_1} \pmod{2^{\epsilon_4 - \epsilon_1 + 1}}. \end{cases}$$

Let $\epsilon_1 = 2$, $\epsilon_2 = 1$, $\epsilon_3 = 1$, $\epsilon_4 = 4$, $\Omega_1 = 3$, $\Delta_1 = 5$, $a_1 = 7$ and $b_2 = q$ an odd prime. By (1.2), $\delta_1 = 15$, $D = 1$, $a_2 = 7$, $\delta_2 = 15$, $\Omega_2 = 1$, $\Omega_3 = 3$ and $D_1 = D_2 = 1$. Since $h_2 = 1$ and

$k_2 = 2$, I, I_2 and I_{21} of (1.5) are applicable, and thus $k' = 2$. By (1.4), $(q|7) = (-30|7) = -1$ since $h = h_2 + h_3 = 1$ and $(q|15\cdot 3\cdot 7) = (-1)^{(q-1)/2\cdot(15\cdot 3\cdot 7 + 1)/2} = 1$ since $k = h_1 + h_3 + k_1 + k_3 = 0$. Thus $(q|7) = -1$ and $(q|5) = -1$. Choose $q = 13$. By (1.7) and (1.9), $26s_1^2 \equiv -15 \pmod{7}$, and thus $s_1 \equiv \pm 2 \pmod{7}$. Choose $s_1 = 2$. Now $a_2 \equiv 7\cdot 3(2\cdot 13\cdot 1\cdot 4 + 15) \equiv 3 \pmod{4}$, which is satisfied by $a_2 = 7$. Thus (1.5) is fulfilled. By $(1.6)_1$, $A_1 = 17$. By (1.8) and (1.10), $3r_1^2 \equiv -17 \pmod{52}$, and thus $r_1 \equiv \pm 9 \pmod{52}$. Choose $r_1 = 9$. By $(1.6)_2$ and (1.11), $c = 5$. By (1.1), $\Omega = 2^2\cdot 3$, $\Delta = 2\cdot 5$, $a = 2\cdot 7$ and $b = 2^6\cdot 3\cdot 13$. By (1.12), $s = D_1 D_2 s_1 = 2$. By (1.13), $r = 2^{\varepsilon_1}\Omega_2\Omega_3 r_1 = 2^2\cdot 3^3$.

$$d = \begin{vmatrix} 2\cdot 7 & 0 & 2 \\ 0 & 2^6\cdot 3\cdot 13 & 2^2\cdot 3^3 \\ 2 & 2^2\cdot 3^3 & 5 \end{vmatrix} = 2^5\cdot 3^2\cdot 5 = \Omega^2\Delta.$$

Since $(a, b, c, r, s) = 1$ and (a, b, c) is odd, the form of this example is properly primitive. Further observe from (3.1) - (3.3) that $n_1 = 1$, $s_1' = 1$; $n_2 = 0$, $r_1' = 9$; $n_3 = 0$, $c' = 5$. Now from the summary of primitive (properly and improperly) forms for subcase $(i)_2$, observe the following:

$P^{(1)}_{ab}$, $P^{(1)}_{ac}$, $P^{(1)}_{ar}$ and $P^{(1)}_{as}$ are not satisfied since a is even, and thus the form of this example is not primitive with (a, bcrs) = 1 and a odd. $P^{(2)}_{ab}$, $P^{(1)}_{bc}$, $P^{(1)}_{br}$ and $P^{(1)}_{bs}$ are not satisfied since b is even, and thus the form of this example is not primitive with (b, acrs) = 1 and b odd. $P^{(2)}_{ar}$, $P^{(2)}_{br}$, $P^{(2)}_{cr}$ and $P^{(1)}_{rs}$ are not satisfied since r is even, and thus the form of this example is not primitive with (r, abcs) = 1 and r odd. $P^{(2)}_{as}$, $P^{(2)}_{bs}$, $P^{(2)}_{cs}$ and $P^{(2)}_{rs}$ are not satisfied since s is even, and thus the form of this example is not primitive with (s, abcr) = 1 and s odd. $P^{(2)}_{ac}$ is satisfied as $n_3 = 0$ and $(a_1, c') = 1$, and thus the form of this example is properly primitive with (a, c) = 1 and c odd. $P^{(2)}_{bc}$ is satisfied as $n_3 = 0$ and $(\Omega_1 b_2, c') = 1$, and thus the form of this example is properly primitive with (b, c) = 1 and c odd. $P^{(1)}_{cr}$ is satisfied as $n_3 = 0$ and $(c', \Omega_1 r'_1) = 1$, and thus the form of this example is properly primitive with (c, r) = 1 and c odd. Finally $P^{(1)}_{cs}$ is satisfied as $n_3 = 0$ and $(c', Ds'_1) = 1$, and thus the form of this example is properly primitive with (c, s) = 1 and c odd.

CHAPTER IV

EXISTENCE OF FORMS IN WHICH $2^n || c_1$ AND EXISTENCE OF FORMS IN WHICH Ω DIVIDES THE COFACTORS OF THE ELEMENTS OF d

Notation: $2^n || c_1$ indicates that $2^n | c_1$ but $2^{n+1} \nmid c_1$.

Lemma 4.1: If (i) $h_1 > 0$ or (ii) $h_3 > 0$ and A_m is odd, $m = 1, 2$ or 3, then $2^{h_2} s_i^2 \not\equiv 0 \pmod 8$, $i = 1, 2$ or 3.

Proof: (i) If $h_1 > 0$, then $h_2 = h_3 = 0$, and thus $(1.6)_1$ reduces to

$$(4.1) \qquad 2^{h_1} a_2 A_m - b_2 D_2 s_i^2 = \delta_2.$$

From (4.1), observe that s_i is odd, and thus $2^{h_2} s_i^2 \not\equiv 0 \pmod 8$.

(ii) If $h_3 > 0$, then $h_1 = h_2 = 0$, and thus $(1.6)_1$ reduces to

$$(4.2) \qquad a_2 A_m - b_2 D_2 s_i^2 = 2^{h_3} \delta_2.$$

Since $h_3 > 0$ and A_m is odd, it follows from (4.2) that $s_i \equiv A_m \equiv 1 \pmod 2$.

Lemma 4.2: If $n \geq 3$ and $w \equiv 1 \pmod 8$, then there exist two solutions of the congruence

(4.3) $x^2 \equiv w \pmod{2^n}$

different from the solutions of the congruence

(4.4) $x^2 \equiv w \pmod{2^{n+1}}$.

Proof: Since $n \geq 3$ and $w \equiv 1 \pmod 8$, each of the congruences (4.3) and (4.4) has four solutions [3]. Let $\pm\alpha$ be a pair of solutions of (4.4). Observe that $\pm\alpha$ is also a pair of solutions of (4.3). Then the other pair of solutions of (4.3) is $\pm(\alpha + 2^{n-1})$. Now $\pm(\alpha + 2^{n-1})$ are not solutions of (4.4), for otherwise, $[\pm(\alpha + 2^{n-1})]^2 \equiv w \pmod{2^{n+1}}$, which implies that

(4.5) $\alpha \equiv 0 \pmod 2$,

since α is a solution of (4.4) and $n \geq 3$. But (4.5) is impossible since α is a solution of (4.3) and w is odd. Thus lemma 4.2 is proved.

Lemma 4.3: If $h_1 = 0$ and $h_2 \geq k_2$, then the congruence (2.5), namely, $s_i^2 \equiv -2^{h_3}\delta_2\alpha \pmod{2^{h_1}a_2}$, where α is defined by (2.6), that is, by $2^{h_2}b_2D_2\alpha \equiv 1 \pmod{2^{h_1}a_2}$ has solutions s_i such that $2^n | s_i$, where $n \geq 1$.

Proof: By (2.13) of theorem 2, the solutions of (2.5) are given by $s_i \equiv \pm\lambda \pmod{2^{h_1}a_2}$, where λ is the least positive residue mod $2^{h_1}a_2$ satisfying (2.5). By (2.1) of theorem 2, we have $s_i = 2^{h_1}a_2\beta \pm \lambda$, where β is arbitrary if $h_2 \geq k_2$.

Note that $(\lambda, 2^{h_1}a_2) = 1$. From (2.1), observe that $2^n | s_i$, where $n \geq 1$ if

$$(4.6) \qquad 2^{h_1}a_2\beta \equiv \mp \lambda (\text{mod } 2^n)$$

has solutions. Each of the congruences (4.6) has no solution or $(2^{h_1}, 2^n)$ solutions according as $(2^{h_1}, 2^n)$ is not or is a divisor of λ. Now $(2^{h_1}, 2^n) = 1$, for otherwise (4.6) will have no solution since $(\lambda , 2^{h_1}) = 1$. Thus (4.6) has no solution or one solution according as $h_1 > 0$ or $h_1 = 0$. This completes the proof of lemma 4.3.

Theorem 4.1: (i) If $k_1 = k_2 = k_3 = 0$, then there exists a form in which c_1 is odd. (ii) If $k_1 = k_3 = 0$ and $2^{h_2}s_i^2 \equiv 0 \ (\text{mod } 8)$, then for any positive integer n, there exists a form in which $2^n || c_1$ if one of the following conditions holds:

$$(4.7) \qquad k_2 + n = 1, \ a_1 \equiv \Delta_1 \ (\text{mod } 4).$$

$$(4.8) \qquad k_2 + n = 2, \ a_1 \equiv 3\Delta_1 \ (\text{mod } 8).$$

$$(4.9) \qquad k_2 + n \geq 3, \ a_1 \equiv 7\Delta_1 \ (\text{mod } 8).$$

Proof: Since $k_1 = k_3 = 0$, from $(1.6)_2$ obtain

$$(4.10) \qquad \Omega_3 r_j^2 \equiv -A_m \ (\text{mod } 2^{k_2}b_2).$$

Define γ by

(4.11) $\Omega_3\gamma \equiv 1 \pmod{2^{k_2}b_2}$.

Now (4.10) and (4.11) yield

(4.12) $r_j^2 \equiv -A_m\gamma \pmod{2^{k_2}b_2}$.

By theorem 2, the solutions of (4.12) are given by

(4.13) $r_j \equiv \pm\,\mu \pmod{2^{k_2}b_2}$,

where μ is the least positive residue mod $2^{k_2}b_2$ satisfying (4.12). From $(1.6)_2$, note that $2^n||c_1$ if r_j satisfies the first and does not satisfy the second of the congruences

(4.14) $\Omega_3 r_j^2 \equiv -A_m \pmod{2^{k_2+g_i}}$, $i = 1, 2;\ g_1 = n,\ g_2 = n + 1$.

Define γ' by

(4.15) $\Omega_3\gamma' \equiv 1 \pmod{2^{k_2+n+1}}$.

Now (4.14) and (4.15) yield

(4.16) $r_j^2 \equiv -A_m\gamma' \pmod{2^{k_2+g_i}}$, $i = 1, 2;\ g_1 = n,\ g_2 = n + 1$.

To prove (i), observe that $k_2 + n = 0$ and (4.16) yield

(4.17) $r_j^2 \equiv -A_m\gamma' \pmod{1}$, $r_j^2 \equiv -A_m\gamma' \pmod{2}$.

It is easily seen that there exist solutions of $(4.17)_1$ which do not satisfy $(4.17)_2$. Further, (4.13) satisfies $(4.17)_1$ and thus $2^0||c_1$, that is, c_1 is odd.

To prove (ii), consider the following three cases.

Case (i): $k_2 + n = 1$. In this case, (4.16) becomes

(4.18) $r_j^2 \equiv -A_m\gamma'$ (mod 2), $r_j^2 \equiv -A_m\gamma'$ (mod 4).

Now $(4.18)_1$ has one solution whereas $(4.18)_2$ has no solution or two solutions according as

(4.19) $-A_m\gamma' \equiv 3$ (mod 4) or $-A_m\gamma' \equiv 1$ (mod 4).

By (4.15) with $k_2 + n = 1$, observe that (4.19) is equivalent to

(4.20) $A_m \equiv \Omega_3$ (mod 4) or $A_m \equiv 3\Omega_3$ (mod 4).

Since A_m is odd by (4.20) and $2^{h_2}s_i^2 \equiv 0$ (mod 8) by hypothesis, it follows from lemma 4.1 that $h_1 = h_3 = 0$. Thus $(1.6)_1$ reduces to

(4.21) $A_m \equiv a_2\delta_2$ (mod 8).

By (1.2) and (4.21), observe that $(4.20)_1$ is equivalent to

(4.22) $a_1 \equiv \Delta_1$ (mod 4),

and thus there exists a solution of $(4.18)_1$ which does not satisfy $(4.18)_2$ if (4.7) holds. Let this solution be given by

(4.23) $r_j \equiv \mu'$ (mod 2).

From (4.13), obtain

(4.24) $r_j \equiv \pm\,\mu$ (mod 2^{k_2}), $r_j \equiv \pm\,\mu$ (mod b_2).

By the Chinese remainder theorem, there exist common solutions of (4.23) and $(4.24)_2$. Let one of these common solutions be given by

(4.25) $r_j \equiv \mu'' \pmod{2b_2}$.

It is easily seen that (4.25) satisfies $(4.24)_1$, and thus (4.25) is one of the common solutions of (4.13) and (4.23).

Case (ii): $k_2 + n = 2$. In this case, (4.16) becomes

(4.26) $r_j^2 \equiv -A_m\gamma' \pmod 4$, $r_j^2 \equiv -A_m\gamma' \pmod 8$.

From case (i), note that $(4.26)_1$ has two solutions if $(4.20)_2$ holds. Observe that (4.21) is valid in this case also since A_m is odd by $(4.20)_2$. By (1.2) and (4.21), observe that $(4.20)_2$ is equivalent to

(4.27) $a_1 \equiv 3\Delta_1 \pmod 4$.

Now $(4.26)_2$ has no solution or four solutions according as

(4.28) $-A_m\gamma' \not\equiv 1 \pmod 8$ or $-A_m\gamma' \equiv 1 \pmod 8$.

By (4.15) with $k_2 + n = 2$, note that $(4.28)_2$ is equivalent to

(4.29) $A_m \equiv 7\Omega_3 \pmod 8$.

By (1.2) and (4.21), observe that (4.29) is equivalent to

(4.30) $a_1 \equiv 7\Delta_1 \pmod 8$,

and thus $(4.26)_2$ has no solution if $a_1 \not\equiv 7\Delta_1 \pmod 8$.

Hence if (4.8) holds, then there exist two solutions of $(4.26)_1$ which do not satisfy $(4.26)_2$. Let one of these solutions be given by

$$(4.31) \qquad r_j \equiv \mu_1 \pmod{4}.$$

By the arguments similar to those in case (i), there exist common solutions of (4.13) and (4.31).

Case (iii): $k_2 + n \geq 3$. In this case, each of the congruences (4.16) has four solutions if (4.30) holds. From lemma 4.2, observe that there exist two solutions of $(4.16)_1$ which do not satisfy $(4.16)_2$. Let one of these solutions be given by

$$(4.32) \qquad r_j \equiv \mu_2 \pmod{2^{k_2+n}}.$$

Again by the arguments similar to those in case (i), there exist common solutions of (4.13) and (4.32).

Theorem 4.2: (i) If $k_1 = 1$ and r_j is odd, then there exists a form in which c_1 is odd. (ii) If $k_1 = 1$, A_m is odd and r_j is even, then there exists a form in which $2||c_1$. (iii) If $k_1 = 1$, then for any integer $n \geq 2$, there exists a form in which $2^n||c_1$ if one of the following conditions holds:

$$h_3 = 1,\ s_i \equiv 2r_j \equiv 0 \pmod 4 \begin{cases} n = 2 \\ n = 3,\ a_1 \equiv \Delta_1 \pmod 4 \\ n = 4,\ a_1 \equiv 3\Delta_1 \pmod 8 \\ n > 4,\ a_1 \equiv 7\Delta_1 \pmod 8). \end{cases}$$

Proof: From the summaries of theorem 1, observe that $k_1 = 0$ or 1. The case $k_1 = 0$ has been discussed in theorem 4.1 and the remaining case $k_1 = 1$ will be discussed in this theorem. Since $k_1 = 1 \Rightarrow k_2 = k_3 = 0$, $(1.6)_2$ yields

(4.33) $\Omega_3 r_j^2 \equiv -2A_m \pmod{b_2}$.

Define γ by

(4.34) $\Omega_3\gamma \equiv 1 \pmod{b_2}$.

Now (4.33) and (4.34) imply that

(4.35) $r_j^2 \equiv -2A_m\gamma \pmod{b_2}$.

By theorem 2, the solutions of (4.35) are given by

(4.36) $r_j \equiv \pm\, \mu \pmod{b_2}$,

where μ is the least positive residue mod b_2 satisfying (4.35). From $(1.6)_2$, note that $2^n || c_1$ if r_j satisfies the first and does not satisfy the second of the congruences

(4.37) $\Omega_3 r_j^2 \equiv -2A_m \pmod{2^{g_i}}$, $i = 1, 2$; $g_1 = n$, $g_2 = n + 1$.

Define γ_1 by

(4.38) $\Omega_3\gamma_1 \equiv 1 \pmod{2^{n+1}}$.

Now (4.37) and (4.38) yield

(4.39) $\quad r_j^2 \equiv -2A_m\gamma_1 \pmod{2^{g_i}}$, $i = 1, 2$; $g_1 = n$, $g_2 = n + 1$.

To prove (i), observe that $n = 0$ and (4.39) imply that $r_j^2 \equiv -2A_m\gamma_1 \pmod{1}$, $r_j^2 \equiv -2A_m\gamma_1 \pmod{2}$, that is,

(4.40) $\quad r_j^2 \equiv -2A_m\gamma_1 \pmod{1}$, $r_j^2 \equiv 0 \pmod{2}$.

Observe from $(4.40)_2$ that r_j is even, and thus there exist solutions of $(4.40)_1$ which do not satisfy $(4.40)_2$ if r_j is odd. Further, (4.36) satisfies $(4.40)_1$.

To prove (ii), observe that $n = 1$ and (4.39) yield $r_j^2 \equiv -2A_m\gamma_1 \pmod{2}$, $r_j^2 \equiv -2A_m\gamma_1 \pmod{4}$, that is,

(4.41) $\quad r_j^2 \equiv 0 \pmod{2}$, $r_j^2 \equiv -2A_m\gamma_1 \pmod{4}$.

Choose s_i such that A_m is odd, which is possible since if $h_3 > 0$, then $(1.6)_1 \Rightarrow A_m \equiv s_i \pmod{2}$, and thus choose $s_i \equiv 1 \pmod{2}$; if $h_1 = h_2 = h_3 = 0$, then choose $s_i \equiv 0 \pmod{2}$; if $h_1 > 0$, $h_2 = h_3 = 0$, then choose s_i such that $2^{h_1} || (b_2D_2s_i^2 + \delta_2)$; and if $h_2 > 0$, $h_1 = h_3 = 0$, then s_i is arbitrary. Observe from $(4.41)_1$ that r_j is even. Thus there exists a solution of $(4.41)_1$ which does not satisfy $(4.41)_2$ if A_m is odd and r_j is even. Let this solution be given by

(4.42) $\quad r_j \equiv \mu_1 \pmod{2}$.

By the Chinese remainder theorem, there exist common solutions of (4.36) and (4.42).

To prove (iii), choose s_i such that

$$(4.43) \qquad A_m = 2A_{m+1},\ A_{m+1} \text{ odd},$$

which is possible, since $(1.6)_1$, (4.43), $h_3 = 1$ and $s_i \equiv 0 \pmod 4$ imply that

$$(4.44) \qquad A_{m+1} \equiv a_2\delta_2 \pmod 8.$$

Since $r_j \equiv 0 \pmod 2$, define r_{j+1} by

$$(4.45) \qquad r_j = 2r_{j+1}.$$

Now from (4.39), (4.43) and (4.45), obtain

$$(4.46) \quad \begin{cases} r_{j+1}^2 \equiv -A_{m+1}\gamma_1 \pmod{2^{g_i-2}}, \\ i = 1,\ 2;\ g_1 = n,\ g_2 = n+1. \end{cases}$$

Case (i): n = 2. Now (4.46) reduces to

$$(4.47) \qquad r_{j+1}^2 \equiv -A_{m+1}\gamma_1 \pmod 1,\ r_{j+1}^2 \equiv -A_{m+1}\gamma_1 \pmod 2.$$

It is easily seen that there exist solutions of $(4.47)_1$ which do not satisfy $(4.47)_2$. Further, (4.36) satisfies $(4.47)_1$.

Case (ii): n = 3. In this case, (4.46) becomes

$$(4.48) \qquad r_{j+1}^2 \equiv -A_{m+1}\gamma_1 \pmod 2,\ r_{j+1}^2 \equiv -A_{m+1}\gamma_1 \pmod 4.$$

Now $(4.48)_1$ has one solution, whereas $(4.48)_2$ has no solution or two solutions according as

(4.49) $\quad -A_{m+1}\gamma_1 \equiv 3 \pmod 4$ or $-A_{m+1}\gamma_1 \equiv 1 \pmod 4$.

By (4.38) with $n = 3$, (4.49) is equivalent to

(4.50) $\quad A_{m+1} \equiv \Omega_3 \pmod 4$ or $A_{m+1} \equiv 3\Omega_3 \pmod 4$.

By (1.2) and (4.44), note that (4.50) is equivalent to

(4.51) $\quad a_1 \equiv \Delta_1 \pmod 4$ or $a_1 \equiv 3\Delta_1 \pmod 4$.

Thus there exists a solution of $(4.48)_1$ which does not satisfy $(4.48)_2$ if $(4.51)_1$ holds. Let this solution be given by

(4.52) $\quad r_{j+1} \equiv \mu_2 \pmod 2$.

By the Chinese remainder theorem, there exist common solutions of (4.36) and (4.52).

Case (iii): n = 4. Now (4.46) reduces to

(4.53) $\quad r_{j+1}^2 \equiv -A_{m+1}\gamma_1 \pmod 4$, $r_{j+1}^2 \equiv -A_{m+1}\gamma_1 \pmod 8$.

From the preceding case, $(4.53)_1$ has two solutions if $(4.51)_2$ holds. Further, $(4.53)_2$ has no solution or four solutions according as

(4.54) $\quad -A_{m+1}\gamma_1 \not\equiv 1 \pmod 8$ or $-A_{m+1}\gamma_1 \equiv 1 \pmod 8$.

By (4.38) with $n = 4$, $(4.54)_2$ is equivalent to

(4.55) $\quad A_{m+1} \equiv 7\Omega_3 \pmod 8$.

By (1.2) and (4.44), note that (4.55) is equivalent to

$a_1 \equiv 7\Delta_1 \pmod 8$, and thus $(4.53)_2$ has no solution if $a_1 \not\equiv 7\Delta_1 \pmod 8$. Hence there exist two solutions of $(4.53)_1$ which do not satisfy $(4.53)_2$ if $a_1 \equiv 3\Delta_1 \pmod 8$. Let one of these solutions be given by

$$(4.56) \qquad r_{j+1} \equiv \mu_3 \pmod 4.$$

By the Chinese remainder theorem, there exist common solutions of (4.36) and (4.56).

Case (iv): $n > 4$. In this case, each of the congruences (4.46) has four solutions if $a_1 \equiv 7\Delta_1 \pmod 8$. By lemma 4.2, there exist two solutions of $(4.46)_1$ which do not satisfy $(4.46)_2$. Let one of these solutions be given by

$$(4.57) \qquad r_{j+1} \equiv \mu_4 \pmod{2^n}$$

Again by the Chinese remainder theorem, there exist common solutions of (4.36) and (4.57).

Theorem 4.3: If $k_3 > 0$, then for any non-negative integer n, there exists a form in which $2^n || c_1$ if one of the following conditions holds:

$$n > k_3,\ h_3 = k_3 \qquad \begin{cases} n - k_3 = 1,\ a_1 \equiv \Delta_1 \pmod{4} \\ n - k_3 = 2,\ a_1 \equiv 3\Delta_1 \pmod{8} \\ n - k_3 \geq 3,\ a_1 \equiv 7\Delta_1 \pmod{8} \end{cases}$$

$$\begin{array}{l} n > k_3,\ h_3 > k_3, \\ k_3 \equiv 0 \pmod{2}, \\ h_3 - k_3 \geq 3 \end{array} \qquad \begin{cases} n - k_3 = 1,\ b_2 \equiv a_1\Omega_1 \pmod{4} \\ n - k_3 = 2,\ b_2 \equiv 3a_1\Omega_1 \pmod{8} \\ n - k_3 \geq 3,\ b_2 \equiv 7a_1\Omega_1 \pmod{8} \end{cases}$$

$\underline{n > k_3,\ h_3 < k_3}$:

$$\begin{array}{l} h_3 > 0, \\ h_3 \equiv 0 \pmod{2} \end{array} \qquad \begin{cases} n - k_3 = 1,\ 2^{k_3-h_3}\Omega_1 \equiv a_1b_2 + a_2\delta_2 \pmod{4} \\ n - k_3 = 2,\ 2^{k_3-h_3}3\Omega_1 \equiv a_1b_2 + a_2\delta_2 \pmod{8} \\ n - k_3 \geq 3,\ 2^{k_3-h_3}7\Omega_1 \equiv a_1b_2 + a_2\delta_2 \pmod{8} \end{cases}$$

$$\begin{array}{l} h_3 = 0, \\ h_1 = h_2 = 0 \end{array} \qquad \begin{cases} n - k_3 = 1,\ 2^{k_3}\Omega_1 \equiv a_1b_2 + a_2\delta_2 \pmod{4} \\ n - k_3 = 2,\ 2^{k_3}3\Omega_1 \equiv a_1b_2 + a_2\delta_2 \pmod{8} \\ n - k_3 \geq 3,\ 2^{k_3}7\Omega_1 \equiv a_1b_2 + a_2\delta_2 \pmod{8} \end{cases}$$

$$\begin{array}{l} h_3 = 0, \\ h_1 > 0, \\ h_2 = 0 \end{array} \qquad \begin{cases} n - k_3 = 1,\ b_2 \equiv 3\delta_1 \pmod{4} \\ n - k_3 = 2,\ 2^{k_3+h_1}3\Omega_1 \equiv a_1b_2 + a_2\delta_2 \pmod{8} \\ n - k_3 \geq 3,\ 2^{k_3+h_1}7\Omega_1 \equiv a_1b_2 + a_2\delta_2 \pmod{8} \end{cases}$$

$$n = k_3 \begin{cases} h_3 = k_3 \\ h_3 > k_3,\ k_3 \equiv 0 \pmod 2 \\ h_3 < k_3 \quad \begin{cases} h_3 > 0,\ h_3 \equiv 0 \pmod 2 \\ h_3 = 0,\ h_1 = h_2 = 0 \\ h_3 = 0,\ h_1 > 0,\ h_2 = 0 \end{cases} \end{cases}$$

$$n < k_3 \begin{cases} h_3 = n = 0 \begin{cases} h_1 = h_2 = 0 \\ h_1 = 0,\ h_2 > 0 \end{cases} \\ h_3 = n > 0 \\ h_3 > n = 0 \\ h_3 > n > 0,\ n \equiv 0 \pmod 2 \\ h_3 < n,\ h_3 > 0,\ h_3 \equiv 0 \pmod 2 \\ \begin{array}{l} h_3 < n \\ h_3 = 0 \end{array} \quad \begin{cases} h_1 = h_2 = 0 \\ h_1 > 0,\ h_2 = 0. \end{cases} \end{cases}$$

Proof: From $(1.6)_2$, we have

(4.58) $$2^{k_3}\Omega_3 r_j^2 \equiv -A_m \pmod{b_2},$$

since $k_3 > 0 \Rightarrow k_1 = k_2 = 0$. Define γ by

(4.59) $$2^{k_3}\Omega_3\gamma \equiv 1 \pmod{b_2}.$$

Now (4.58) and (4.59) yield

(4.60) $$r_j^2 \equiv -A_m\gamma \pmod{b_2}.$$

By theorem 2, the solutions of (4.60) are given by

(4.61) $$r_j \equiv \pm\,\mu \pmod{b_2},$$

where μ is the least positive residue mod b_2 satisfying (4.60). From $(1.6)_2$, note that $2^n || c_1$ if r_j satisfies the first and does not satisfy the second of the congruences

(4.62) $$2^{k_3}\Omega_3 r_j^2 \equiv -A_m \pmod{2^{g_i}},\ i = 1, 2;\ g_1 = n,\ g_2 = n + 1.$$

Case (i): $n > k_3$. It will be seen that s_i can be chosen such that

(4.63) $$A_m = 2^{k_3}A_{m+1},\ A_{m+1} \text{ odd}.$$

Now from (4.62) and (4.63), obtain

(4.64) $$\begin{cases} \Omega_3 r_j^2 \equiv -A_{m+1} \pmod{2^{g_i-k_3}},\ i = 1, 2; \\ g_1 = n,\ g_2 = n + 1. \end{cases}$$

Define γ_2 by

(4.65) $\quad \Omega_3\gamma_2 \equiv 1 \pmod{2^{n-k_3+1}}$.

From (4.64) and (4.65), we have

$$(4.66) \quad \begin{cases} r_j^2 \equiv -A_{m+1}\gamma_2 \pmod{2^{g_i-k_3}}, \\ i = 1,\ 2;\ g_1 = n,\ g_2 = n+1. \end{cases}$$

From $(1.6)_1$ and (4.63), obtain

(4.67) $\quad 2^{h_1+k_3}a_2A_{m+1} - 2^{h_2}b_2D_2s_i^2 = 2^{h_3}\delta_2$.

Case $(i)_1$: $h_3 = k_3$. If h_3 is even, by lemma 4.3, choose s_i such that

(4.68) $\quad s_i \equiv 0 \pmod{2^{(h_3+4)/2}}$.

If h_3 is odd, again by lemma 4.3, choose s_i such that

(4.69) $\quad s_i \equiv 0 \pmod{2^{(h_3+3)/2}}$.

Using (4.68) or (4.69) as the case may be in (4.67), we have

(4.70) $\quad A_{m+1} \equiv a_2\delta_2 \pmod 8$

and thus s_i can be chosen such that (4.63) is satisfied.

Case $(i)_{11}$: $n - k_3 = 1$. In this case, (4.66) becomes

(4.71) $\quad r_j^2 \equiv -A_{m+1}\gamma_2 \pmod 2,\ r_j^2 \equiv -A_{m+1}\gamma_2 \pmod 4$.

Now $(4.71)_1$ has one solution, whereas $(4.71)_2$ has no solution or two solutions according as

(4.72) $\quad -A_{m+1}\gamma_2 \equiv 3 \pmod 4$ or $-A_{m+1}\gamma_2 \equiv 1 \pmod 4$.

Further, by (4.65) with $n - k_3 = 1$, (4.72) is equivalent to

(4.73) $\quad A_{m+1} \equiv \Omega_3 \pmod 4$ or $A_{m+1} \equiv 3\Omega_3 \pmod 4$.

By (1.2) and (4.70), observe that (4.73) is equivalent to

(4.74) $\quad a_1 \equiv \Delta_1 \pmod 4$ or $a_1 \equiv 3\Delta_1 \pmod 4$.

Thus there exists a solution of $(4.71)_1$ which does not satisfy $(4.71)_2$ if $n > k_3$, $h_3 = k_3$, $n - k_3 = 1$ and $a_1 \equiv \Delta_1 \pmod 4$. Let this solution be given by

(4.75) $\quad r_j \equiv \mu' \pmod 2$.

By the Chinese remainder theorem, there exist common solutions of (4.61) and (4.75).

Case $(i)_{12}$: $n - k_3 = 2$. Now (4.66) reduces to

(4.76) $\quad r_j^2 \equiv -A_{m+1}\gamma_2 \pmod 4$, $r_j^2 \equiv -A_{m+1}\gamma_2 \pmod 8$.

From the preceding case, note that $(4.76)_1$ has two solutions if $(4.74)_2$ holds. By the arguments similar to those in case (iii) of theorem 4.2 (iii), $(4.76)_2$ has no solution if $a_1 \not\equiv 7\Delta_1 \pmod 8$. Thus there exist two solutions of $(4.76)_1$ which do not satisfy $(4.76)_2$ if $n > k_3$, $h_3 = k_3$, $n - k_3 = 2$ and $a_1 \equiv 3\Delta_1 \pmod 8$. The rest of the discussion is similar to that of the previous case.

Case $(i)_{13}$: $n - k_3 \geq 3$. In this case, each of the congruences (4.66) has four solutions if $a_1 \equiv 7\Delta_1 \pmod 8$ and the rest of the discussion is similar to that of case (iv) of theorem 4.2 (iii).

Case $(i)_2$: $h_3 > k_3$. If k_3 is even, by lemma 4.3, choose s_i such that

$$(4.77) \qquad s_i = 2^{k_3/2} s_{i+1},\ s_{i+1} \text{ odd},$$

which is possible since $2^q || s_i$, that is, $a_2\beta = 2^q\eta \mp \lambda \not\equiv \mp \lambda$ (mod 2^{q+1}) iff $\eta \equiv 1 \pmod 2$ and note that there always exists η such that $2^q\eta \equiv \pm \lambda$ (mod a_2) and $\eta \equiv 1 \pmod 2$. From (4.67) and (4.77), obtain

$$(4.78) \qquad A_{m+1} \equiv a_2(b_2D_2 + 2^{h_3-k_3}\delta_2) \pmod 8.$$

By (1.2) and (4.78), we have

$$(4.79) \qquad A_{m+1} \equiv a_1b_2 + 2^{h_3-k_3}a_2\delta_2 \pmod 8.$$

Since $h_3 - k_3 \geq 3$, (4.79) reduces to

$$(4.80) \qquad A_{m+1} \equiv a_1b_2 \pmod 8,$$

and thus s_i can be chosen such that (4.63) holds.

Similarly if k_3 is odd, choose s_i such that $s_i = 2^{(k_3+1)/2} s_{i+1}$, s_{i+1} odd, and thus (4.67) yields $a_2A_{m+1} - 2b_2D_2s_{i+1}^2 = 2^{h_3-k_3}\delta_2$, which implies that A_{m+1} is even. Thus it is impossible to choose s_i such that (4.63) holds if k_3 is odd.

Case $(i)_{21}$: $n - k_3 = 1$. This case is similar to $(i)_{11}$. By (1.2) and (4.80), observe that (4.73) is equivalent to

$$(4.81) \qquad b_2 \equiv a_1\Omega_1 \pmod 4 \text{ or } b_2 \equiv 3a_1\Omega_1 \pmod 4.$$

The rest of the discussion is similar to that of case $(i)_{11}$.

Case $(i)_{22}$: $n - k_3 = 2$. This is similar to case $(i)_{12}$.

Case $(i)_{23}$: $n - k_3 \geq 3$. This is similar to $(i)_{13}$.

Case $(i)_{31}$: $0 < h_3 < k_3$. As in case $(i)_2$, if h_3 is even, choose s_i such that

$$(4.82) \qquad s_i = 2^{h_3/2} s_{i+1}, \; s_{i+1} \text{ odd}.$$

From (4.67) and (4.82), obtain

$$(4.83) \qquad 2^{k_3-h_3}A_{m+1} \equiv a_2(b_2D_2 + \delta_2) \pmod 8.$$

Now by (1.2) and (4.83), we have

$$(4.84) \qquad 2^{k_3-h_3}A_{m+1} \equiv a_1b_2 + a_2\delta_2 \pmod 8.$$

Similarly if h_3 is odd, choose s_i such that $s_i = 2^{(h_3+1)/2} s_{i+1}$, s_{i+1} odd, and thus (4.67) yields $2^{k_3-h_3}a_2A_{m+1} - 2b_2D_2s_{i+1}^2 = \delta_2$, which is impossible since δ_2 is odd.

Case $(i)_{311}$: $n - k_3 = 1$. This is similar to $(i)_{11}$. By (1.2) and (4.84), observe that (4.73) is equivalent to

$$(4.85)\quad \begin{cases} 2^{k_3-h_3}\Omega_1 \equiv a_1b_2 + a_2\delta_2 \pmod 4 \text{ or} \\ 2^{k_3-h_3}3\Omega_1 \equiv a_1b_2 + a_2\delta_2 \pmod 4. \end{cases}$$

The rest of the discussion is similar to that of $(i)_{11}$.

Case $(i)_{312}$: $n - k_3 = 2$. This is similar to $(i)_{12}$.

Case $(i)_{313}$: $n - k_3 \geq 3$. This is similar to $(i)_{13}$.

Case $(i)_{321}$: $0 = h_3 < k_3$, $h_1 = h_2 = 0$. From (1.2) and (4.67), obtain

$$(4.86)\quad 2^{k_3}A_{m+1} \equiv a_1b_2 + a_2\delta_2 \pmod 8.$$

Case $(i)_{3211}$: $n - k_3 = 1$. This is similar to $(i)_{11}$. By (1.2) and (4.86), note that (4.73) is equivalent to

$$(4.87)\quad \begin{cases} 2^{k_3}\Omega_1 \equiv a_1b_2 + a_2\delta_2 \pmod 4 \text{ or} \\ 2^{k_3}3\Omega_1 \equiv a_1b_2 + a_2\delta_2 \pmod 4. \end{cases}$$

The rest of the discussion is similar to that of $(i)_{11}$.

Case $(i)_{3212}$: $n - k_3 = 2$. This is similar to $(i)_{12}$.

Case $(i)_{3213}$: $n - k_3 \geq 3$. This is similar to $(i)_{13}$.

Case $(i)_{322}$: $0 = h_3 < k_3$, $h_1 = 0$, $h_2 > 0$. By (4.67), obtain $2^{k_3}a_2A_{m+1} - 2^{h_2}b_2D_2s_i^2 = \delta_2$, which is impossible, and thus this case is impossible.

Case $(i)_{323}$: $0 = h_3 < k_3$, $h_1 > 0$, $h_2 = 0$. From (1.2) and

(4.67), obtain

$$(4.88) \qquad 2^{k_3+h_1}A_{m+1} \equiv a_1b_2 + a_2\delta_2 \pmod 8.$$

Case $(i)_{3231}$: $n - k_3 = 1$. This is similar to $(i)_{11}$. By (1.2) and (4.88), observe that (4.73) is equivalent to

$$(4.89) \quad \begin{cases} 2^{k_3+h_1}\Omega_1 \equiv a_1b_2 + a_2\delta_2 \pmod 4 \text{ or} \\ 2^{k_3+h_1}3\Omega_1 \equiv a_1b_2 + a_2\delta_2 \pmod 4. \end{cases}$$

Since $h_1 > 0$ and $k_3 > 0$, $h_1 + k_3$ is at least 2, and thus $(4.89)_1$ reduces to $a_1b_2 + a_2\delta_2 \equiv 0 \pmod 4$, which yields by (1.2), $b_2 \equiv 3\delta_1 \pmod 4$. The rest of the discussion is similar to that of $(i)_{11}$.

Case $(i)_{3232}$: $n - k_3 = 2$. This is similar to $(i)_{12}$.

Case $(i)_{3233}$: $n - k_3 \geq 3$. This is similar to $(i)_{13}$.

Case (ii): $n = k_3$. Choose s_i such that (4.63) holds, which is possible by case (i). Then from (4.62) and (4.63), obtain

$$(4.90) \qquad \Omega_3r_j^2 \equiv -A_{m+1} \pmod 1, \quad \Omega_3r_j^2 \equiv -A_{m+1} \pmod 2,$$

where A_{m+1} is given by (4.70), (4.79), (4.84), (4.86) and (4.88) according as $h_3 = k_3$; $h_3 > k_3$, $k_3 \equiv 0 \pmod 2$; $h_3 < k_3$, $h_3 > 0$, $h_3 \equiv 0 \pmod 2$; $h_3 < k_3$, $h_3 = 0$, $h_1 = h_2 = 0$, and $h_3 < k_3$, $h_3 = 0$, $h_1 > 0$, $h_2 = 0$. Note that there exist solutions of $(4.90)_1$ which do not satisfy $(4.90)_2$. Further, (4.61) satisfies $(4.90)_1$.

Case (iii): $n < k_3$. It will be seen that s_i can be chosen such that

(4.91) $$A_m = 2^n A_{m+1},\ A_{m+1} \text{ odd}.$$

Now from (4.62) and (4.91), obtain

(4.92) $$2^{k_3-n}\Omega_3 r_j^2 \equiv -A_{m+1} \pmod 1,\ 2^{k_3-n}\Omega_3 r_j^2 \equiv -A_{m+1} \pmod 2.$$

Again observe here that there exist solutions of $(4.92)_1$ which do not satisfy $(4.92)_2$. Further (4.61) satisfies $(4.92)_1$.

To determine A_{m+1} in (4.91), from $(1.6)_1$ and (4.91), obtain

(4.93) $$2^{h_1+n} a_2 A_{m+1} - 2^{h_2} b_2 D_2 s_i^2 = 2^{h_3}\delta_2.$$

Case $(\text{iii})_{11}$: $h_3 = n = 0$. Now the following three subcases arise.

Case $(\text{iii})_{111}$: $h_1 = h_2 = 0$. Now (4.93) reduces to

(4.94) $$a_2 A_{m+1} - b_2 D_2 s_i^2 = \delta_2,$$

which yields (4.70), and thus s_i can be chosen such that (4.91) holds.

Case $(\text{iii})_{112}$: $h_1 > 0$, $h_2 = 0$. In this case, (4.93) becomes $2^{h_1} a_2 A_{m+1} - b_2 D_2 s_i^2 = \delta_2$, which yields $2^{h_1} A_{m+1} \equiv a_2\delta_2 \pmod 8$, which is absurd, and thus this case is impossible.

Case $(iii)_{113}$: $h_1 = 0$, $h_2 > 0$. Now (4.93) reduces to

$$(4.95) \qquad a_2A_{m+1} - 2^{h_2}b_2D_2s_i^2 = \delta_2.$$

By lemma 4.3, choose s_i such that $s_i \equiv 0 \pmod 2$, and thus (4.95) yields (4.70), and thus s_i can be chosen such that (4.91) holds.

Case $(iii)_{12}$: $h_3 = n > 0$. In this case, (4.93) becomes

$$(4.96) \qquad 2^na_2A_{m+1} - b_2D_2s_i^2 = 2^n\delta_2.$$

By lemma 4.3, choose s_i such that

$$(4.97) \qquad s_i \equiv 0 \pmod{2^{(n+4)/2}} \text{ or } s_i \equiv 0 \pmod{2^{(n+3)/2}}$$

according as n is even or odd and then (4.96) yields (4.70). Thus s_i can be chosen such that (4.91) holds.

Case $(iii)_{21}$: $h_3 > n = 0$. Now (4.93) becomes

$$(4.98) \qquad a_2A_{m+1} - b_2D_2s_i^2 = 2^{h_3}\delta_2,$$

from which it follows that $s_i \equiv A_{m+1} \pmod 2$, and thus s_i can be chosen such that (4.91) holds.

Case $(iii)_{22}$: $h_3 > n > 0$. In this case, (4.93) becomes

$$(4.99) \qquad 2^na_2A_{m+1} - b_2D_2s_i^2 = 2^{h_3}\delta_2.$$

As in case $(i)_2$, if n is even, choose s_i such that

$$(4.100) \qquad s_i = 2^{n/2}s_{i+1},\ s_{i+1} \text{ odd}.$$

Now (1.2), (4.99) and (4.100) yield

(4.101) $A_{m+1} \equiv a_1b_2 + 2^{h_3-n}a_2\delta_2 \pmod 8$,

and thus s_i can be chosen such that (4.91) holds.

Similarly if n is odd, choose s_i such that $s_i = 2^{(n+1)/2}s_{i+1}$, s_{i+1} odd,and thus (4.99) yields $a_2A_{m+1} - 2b_2D_2s_{i+1}^2 = 2^{h_3-n}\delta_2$, which implies that A_{m+1} is even. Thus it is impossible to choose s_i such that (4.91) holds if n is odd.

Case $(iii)_{31}$: $0 < h_3 < n$. Now (4.93) becomes

(4.102) $2^na_2A_{m+1} - b_2D_2s_i^2 = 2^{h_3}\delta_2$.

Again as in case $(i)_2$, if h_3 is even, choose s_i such that

(4.103) $s_i = 2^{h_3/2}s_{i+1}$, s_{i+1} odd.

Now (1.2), (4.102) and (4.103) yield

(4.104) $2^{n-h_3}A_{m+1} \equiv a_1b_2 + a_2\delta_2 \pmod 8$.

Similarly if h_3 is odd, choose s_i such that $s_i = 2^{(h_3+1)/2}s_{i+1}$, s_{i+1} odd and then (4.102) yields $2^{n-h_3}a_2A_{m+1} - 2b_2D_2s_{i+1}^2 = \delta_2$, which is impossible since δ_2 is odd.

Case $(\mathrm{iii})_{32}$: $0 = h_3 < n$: Now the following three subcases arise.

Case $(\mathrm{iii})_{321}$: $h_1 = h_2 = 0$. By (1.2) and (4.93), obtain

$$(4.105) \qquad 2^n A_{m+1} \equiv a_1 b_2 + a_2 \delta_2 \pmod 8.$$

Case $(\mathrm{iii})_{322}$: $h_1 = 0$, $h_2 > 0$. From (4.93), obtain $2^n a_2 A_{m+1} - 2^{h_2} b_2 D_2 s_i^2 = \delta_2$, which is impossible since δ_2 is odd,and thus this case is impossible.

Case $(\mathrm{iii})_{323}$: $h_1 > 0$, $h_2 = 0$. By (1.2) and (4.93), obtain

$$(4.106) \qquad 2^{h_1+n} A_{m+1} \equiv a_1 b_2 + a_2 \delta_2 \pmod 8.$$

Some examples illustrating theorems 4.1 - 4.3:

Example 4.1: [For theorem 4.1 and subcase $(\mathrm{ii})_{13}$ of theorem 1]

$$\begin{cases} \varepsilon_4 \le \varepsilon' \le \varepsilon_3,\ \varepsilon_4 \ne \varepsilon_3,\ \varepsilon_4 \le \varepsilon_1,\ \varepsilon_4 \equiv \varepsilon' \pmod 2,\ h_1 = \varepsilon_4 - \varepsilon_5, \\ k_3 = \varepsilon_1 - \varepsilon_4,\ A = 2^{\varepsilon_4} A_1,\ s_1 = 2^{[(\varepsilon' - \varepsilon_4 + 1)/2]} s_2,\ s_2 \text{ odd} \\ \text{if } \varepsilon_5 < \varepsilon_4,\ A_1 \equiv 0 \text{ or } 1 \pmod 2 \text{ according as } s_2 \text{ is} \\ \text{chosen to satisfy } b_2 D_2 s_2^2 + \delta_2 \equiv 0 \text{ or } 2^{\varepsilon_4 - \varepsilon_5} \pmod{2^{\varepsilon_4 - \varepsilon_5 + 1}}, \\ c \equiv A_1 + 2^{\varepsilon_1 - \varepsilon_4} r_1 \pmod 2. \end{cases}$$

Let $\varepsilon_1 = 1$, $\varepsilon_2 = 2$, $\varepsilon_3 = 3$, $\varepsilon_4 = 1$, $\Omega_1 = 7$, $\Delta_1 = 5$, $a_1 = 3$ and $b_2 = q$ an odd prime. By (1.2), $\delta_1 = 35$, $D = 1$, $a_2 = 3$, $\delta_2 = 35$, $\Omega_2 = 1$, $\Omega_3 = 7$ and $D_1 = D_2 = 1$; $h_1 = 1$, $k_1 = k_2 = k_3 = 0$. By (1.4), $(q|3) = (-35|3) = 1$ since

$h = h_2 + h_3 = 0$ and $(q|35\cdot 7\cdot 3)$
$= (-1)^{(q-1)/2\cdot(35\cdot 7\cdot 3 + 1)/2}(2|q) = (2|q) = (-1)^{(q^2-1)/8}$
since $k = h_1 + h_3 + k_1 + k_3 = 1$. Thus $(q|3) = 1$ and $(q|5) = (-1)^{(q^2-1)/8}$. Take $q = 13$. By (1.7) and (1.9), $13s_2^2 \equiv -35 \pmod 6$, and thus $s_2 \equiv \pm 1 \pmod 6$. Take $s_2 = 1$. Now $s_1 = 2^{[(\varepsilon'-\varepsilon_4+1)/2]}s_2 = 2s_2 = 2$. By $(1.6)_1$, $A_1 = 8$. By (1.8) and (1.10), $7r_1^2 \equiv -8 \pmod{13}$, and thus $r_1 \equiv \pm 6 \pmod{13}$. This example illustrates the first part of theorem 4.1 as $k_1 = k_2 = k_3 = 0$. By (4.15), $\gamma' \equiv 1 \pmod 2$. Take $\gamma' = 1$. By $(4.17)_2$, $r_1^2 \equiv -8 \pmod 2$, that is, $r_1 \equiv 0 \pmod 2$, and thus choose $r_1 = 7$ which satisfies $r_1 \equiv \pm 6(13)$ and does not satisfy $r_1 \equiv 0 \pmod 2$. By (1.11), $c = c_1$. By $(1.6)_2$, $c_1 = 27$, and thus c_1 is odd as asserted by theorem 4.1 (i). By (1.1), $\Omega = 2\cdot 7$, $\Delta = 2^2\cdot 5$, $a = 2^3\cdot 3$ and $b = 2^2\cdot 7\cdot 13$. By (1.12), $s = D_1D_2s_1 = 2$. By (1.13), $r = 2^{\varepsilon_1}\Omega_2\Omega_3r_1 = 2\cdot 7^2$.

$$d = \begin{vmatrix} 2^3\cdot 3 & 0 & 2 \\ 0 & 2^2\cdot 7\cdot 13 & 2\cdot 7^2 \\ 2 & 2\cdot 7^2 & 3^3 \end{vmatrix} = 2^4\cdot 5\cdot 7^2 = \Omega^2\Delta.$$

Example 4.2: [For theorem 4.1 and subcase $(i)_{51}$ of theorem 1]

$$\left\{\begin{array}{l} \varepsilon_3 \le \varepsilon' \le \varepsilon_4,\ \varepsilon_3 < \varepsilon_2,\ \varepsilon_5 < \varepsilon_4,\ \varepsilon_3 \equiv \varepsilon_2 \pmod 2,\ h_2 = \varepsilon_4 - \varepsilon', \\ k_2 = \varepsilon_4 - \varepsilon_5,\ A = 2^{\varepsilon_5}A_1,\ r_1 = 2^{(\varepsilon_2-\varepsilon_3)/2} r_2,\ A_1r_2 \text{ odd if} \\ \varepsilon_4 > \varepsilon';\ A_1r_2 \equiv s_1 + 1 \equiv 1 \pmod 2 \text{ or } (A_1/4)(r_2/2)s_1 \\ \equiv 1 \pmod 2 \text{ if } \varepsilon_4 = \varepsilon';\ c \equiv 0 \text{ or } 1 \pmod 2 \text{ according as} \\ r_2 \text{ satisfies } \Omega_3 r_2^2 + A_1 \equiv 0 \text{ or } 2^{\varepsilon_4-\varepsilon_5} \pmod{2^{\varepsilon_4-\varepsilon_5+1}}. \end{array}\right.$$

Let $\varepsilon_1 = 1$, $\varepsilon_2 = 2$, $\varepsilon_3 = 0$, $\varepsilon_4 = 4$, $\Omega_1 = 7$, $\Delta_1 = 5$, $a_1 = 3$ and $b_2 = q$ an odd prime. By (1.2), $\delta_1 = 35$, $D = 1$, $a_2 = 3$, $\delta_2 = 35$, $\Omega_2 = 1$, $\Omega_3 = 7$ and $D_1 = D_2 = 1$; $h_2 = k_2 = 1$; By (1.4), $(q|3) = (-70|3) = -1$ since $h = h_2 + h_3 = 1$ and $(q|35\cdot7\cdot3) = (-1)^{(q-1)/2\cdot(35\cdot7\cdot3+1)/2} = 1$ since $k = h_1 + h_3 + k_1 + k_3 = 0$. Thus $(q|3) = (q|5) = -1$. Take $q = 17$. By (1.7) and (1.9), $34s_1^2 \equiv -35 \pmod 3$, and thus $s_1 \equiv \pm 1 \pmod 3$. Choose $s_1 = 4$ so that $2^{h_2}2s_1^2 \equiv 0 \pmod 8$, one of the hypotheses of theorem 4.1 (ii). By $(1.6)_1$, $A_1 = 193$. By (1.8) and (1.10), $7r_2^2 \equiv -193 \pmod{34}$, and thus $r_2 \equiv \pm 15 \pmod{34}$. This example illustrates the second part of theorem 4.1 as $k_1 = k_3 = 0$. Let $k_2 + n = 3$, and thus $n = 2$. Hence we seek c_1 such that $2^2||c_1$. By (4.15), $\gamma' \equiv 7 \pmod{16}$. Choose $\gamma' = 7$. By (4.16), choose r_2 such that it satisfies $r_2^2 \equiv -A_1\gamma' \pmod 8$ and does not satisfy $r_2^2 \equiv -A_1\gamma'$ (mod 16); that is, r_2 satisfies $r_2^2 \equiv 1$ (mod 8) and does not satisfy $r_2^2 \equiv 9$ (mod 16). Choose $r_2 = 15$. By (1.11), $c = c_1$. By $(1.6)_2$, $c_1 = 52$, and thus $2^2 || c_1$ as asserted by theorem 4.1 (ii). By (1.1), $\Omega = 2\cdot 7$, $\Delta = 2^2\cdot 5$, $a = 3$ and $b = 2^5\cdot 7\cdot 17$. By (1.12), $s = D_1D_2s_1 = 2^2$. By (1.13), $r = 2^{\epsilon_1}\Omega_2\Omega_3 r_1 = 2^2\cdot 3\cdot 5\cdot 7$ since $r_1 = 2^{(\epsilon_2-\epsilon_3)/2} r_2 = 2r_2 = 2\cdot 3\cdot 5$.

$$d = \begin{vmatrix} 3 & 0 & 2^2 \\ 0 & 2^5\cdot 7\cdot 17 & 2^2\cdot 3\cdot 5\cdot 7 \\ 2^2 & 2^2\cdot 3\cdot 5\cdot 7 & 2^2\cdot 13 \end{vmatrix} = 2^4\cdot 5\cdot 7^2 = \Omega^2\Delta.$$

Example 4.3: [For theorem 4.2 and subcase $(\text{iv})_{14221}$ of theorem 1]

$$\begin{cases} \epsilon_4 < \epsilon_3 < \epsilon', \ \epsilon_4 = \epsilon_1, \ 1 \le \epsilon_4 < \epsilon_5, \ 0 \equiv \epsilon_4 \equiv \epsilon_3 + 1 \pmod 2, \\ h_3 = (\epsilon_5 - 1) - \epsilon_4, \ k_1 = 1, \ A = 2^{\epsilon_4+1}A_3, \ s_1 = 2^{(\epsilon_3+1)/2}s_3, \\ A_3 \equiv s_3 + 2^{(\epsilon_5-1)-\epsilon_4} \pmod 2, \ c \equiv r_1 \pmod 2). \end{cases}$$

Let $\epsilon_1 = 2$, $\epsilon_2 = 4$, $\epsilon_3 = 3$, $\epsilon_4 = 2$, $\Omega_1 = 3$, $\Delta_1 = 5$, $a_1 = 7$ and $b_2 = q$ an odd prime. By (1.2), $\delta_1 = 15$, $D = 1$, $a_2 = 7$, $\delta_2 = 15$, $\Omega_2 = 1$, $\Omega_3 = 3$ and $D_1 = D_2 = 1$; $h_1 = h_2 = h_3 = 0$, $k_1 = 1$. By (1.4), $(q|7) = (-15|7) = -1$ since $h = h_2 + h_3 = 0$ and $(q|15\cdot 3\cdot 7) = (-1)^{(q-1)/2\cdot(15\cdot 3\cdot 7 + 1)/2}(2|q) = (2|q)$

$= (-1)^{(q^2-1)/8}$ since $k = h_1 + h_3 + k_1 + k_3 = 1$. Thus $(q|7) = -1$ and $(q|5) = (-1)^{(q^2+7)/8}$. Choose $q = 17$. By (1.7) and (1.9), $17s_3^2 \equiv -15 \pmod 7$, and thus $s_3 \equiv \pm 3 \pmod 7$. Choose $s_3 = 3$. Then $s_1 = 2^{(\epsilon_3+1)/2} s_3 = 4s_3 = 2^2\cdot 3$. By $(1.6)_1$, $A_3 = 24$. By (1.8) and (1.10), $3r_1^2 \equiv -48 \pmod{17}$, and thus $r_1 \equiv \pm 1 \pmod{17}$. Choose $r_1 = 1$ so that this example illustrates the first part of theorem 4.2. By (1.11), $c = c_1$. By $(1.6)_2$, $c_1 = 3$, and thus c_1 is odd as asserted by theorem 4.2 (i). By (1.1), $\Omega = 2^2\cdot 3$, $\Delta = 2^4\cdot 5$, $a = 2^3\cdot 7$ and $b = 2^4\cdot 3\cdot 17$. By (1.12), $s = D_1 D_2 s_1 = 2^2\cdot 3$. By (1.13), $r = 2^{\epsilon_1}\Omega_2\Omega_3 r_1 = 2^2\cdot 3$.

$$d = \begin{vmatrix} 2^3\cdot 7 & 0 & 2^2\cdot 3 \\ 0 & 2^4\cdot 3\cdot 17 & 2^2\cdot 3 \\ 2^2\cdot 3 & 2^2\cdot 3 & 3 \end{vmatrix} = 2^8\cdot 3^2\cdot 5 = \Omega^2\Delta.$$

Example 4.4: [For theorem 4.2 and subcase $(iv)_{14221}$ of theorem 1]

Summary of subcase $(iv)_{14221}$ is given in example 4.3.

Let $\epsilon_1 = 2$, $\epsilon_2 = 5$, $\epsilon_3 = 3$, $\epsilon_4 = 2$, $\Omega_1 = 3$, $\Delta_1 = 5$ and $b_2 = q$ an odd prime. $h_3 = 1$ and $k_1 = 1$. Let $n = 4$, that is, we seek c_1 such that $2^4 || c_1$. Choose a_1 such that

$a_1 \equiv 3\Delta_1 \pmod{8}$. Let $a_1 = 7$. By (1.2), $\delta_1 = 15$, $D = 1$, $a_2 = 7$, $\delta_2 = 15$, $\Omega_2 = 1$, $\Omega_3 = 3$ and $D_1 = D_2 = 1$. By (1.4), $(q|7) = (-30|7) = -1$ since $h = h_2 + h_3 = 1$ and $(q|15\cdot 3\cdot 7) = (-1)^{(q-1)/2\cdot(15\cdot 3\cdot 7 + 1)/2} = 1$ since $k = h_1 + h_3 + k_1 + k_3 = 2$. Thus $(q|5) = (q|7) = -1$. Choose $q = 13$. By (1.7) and (1.9), $13s_3^2 \equiv -30 \pmod{7}$, and thus $s_3 \equiv \pm 3 \pmod{7}$. Choose s_3 such that $s_3 \equiv 0 \pmod{4}$. Take $s_3 = 4$. $s_1 = 2^{(\varepsilon_3+1)/2} s_3 = 4s_3 = 2^4$. By $(1.6)_1$, $A_3 = 34$. By (1.8) and (1.10), $3r_1^2 \equiv -68 \pmod{13}$, and thus $r_1 \equiv \pm 5 \pmod{13}$. Choose r_1 such that $r_1 \equiv 0 \pmod{2}$. By (4.38), $3\gamma_1 \equiv 1 \pmod{32}$, and thus $\gamma_1 \equiv 11 \pmod{32}$. Take $\gamma_1 = 11$. By (4.43), $A_4 = 17$. By $(4.53)_1$, $r_2^2 \equiv -187 \pmod{4}$, and thus $r_2 \equiv \pm 1 \pmod{4}$. $r_1 = 2r_2$ by (4.45). Choose $r_1 = 18$ to satisfy all the preceding conditions on r_1 and r_2. By (1.11), $c = c_1$. By $(1.6)_2$, $c_1 = 2^4\cdot 5$, and thus $2^4 || c_1$ as asserted by theorem 4.2 (iii). By (1.1), $\Omega = 2^2\cdot 3$, $\Delta = 2^5\cdot 5$, $a = 2^3\cdot 7$ and $b = 2^4\cdot 3\cdot 13$. By (1.12), $s = D_1D_2s_1 = 2^4$. By (1.13), $r = 2^{\varepsilon_1}\Omega_2\Omega_3 r_1 = 2^3\cdot 3^3$.

$$d = \begin{vmatrix} 2^3\cdot 7 & 0 & 2^4 \\ 0 & 2^4\cdot 3\cdot 13 & 2^3\cdot 3^3 \\ 2^4 & 2^3\cdot 3^3 & 2^4\cdot 5 \end{vmatrix} = 2^9\cdot 3^2\cdot 5 = \Omega^2\Delta.$$

Example 4.5: [For theorem 4.3 and subcase $(iii)_{111}$ of theorem 1]

$$\begin{cases} \epsilon_3 \le \epsilon_4 < \epsilon', \ \epsilon_4 \le \epsilon_1, \ \epsilon_4 \le \epsilon_5, \ \epsilon_3 \equiv 0 \pmod 2, \ h_3 = \\ \epsilon_5 - \epsilon_4, \ k_3 = \epsilon_1 - \epsilon_4, \ A = 2^{\epsilon_4} A_2, \ s_1 = 2^{\epsilon_3/2} s_2, \ A_2 \\ \equiv s_2 + 2^{\epsilon_5 - \epsilon_4} \pmod 2, \ c \equiv A_2 + 2^{\epsilon_1 - \epsilon_4} r_1 \pmod 2. \end{cases}$$

Let $\epsilon_1 = 3$, $\epsilon_2 = 3$, $\epsilon_3 = 0$, $\epsilon_4 = 1$, $\Omega_1 = 3$, $\Delta_1 = 5$, $a_1 = 7$.

$h_3 = 5$ and $k_3 = 2$. Let $n = 3$, that is, we seek c_1 such that $2^3 || c_1$. $n - k_3 = 1$. Choose $b_2 = q$ an odd prime such that $b_2 \equiv a_1\Omega_1 \pmod 4$. $n > k_3$, $h_3 > k_3$, $k_3 \equiv 0 \pmod 2$ and $h_3 - k_3 = 3$. By (1.4), $(q|7) = (-480|7) = -1$ since $h = h_2 + h_3 = 5$ and $(q|15\cdot 3\cdot 7) = (-1)^{(q-1)/2\cdot(15\cdot 3\cdot 7 + 1)/2}$ $(2^7|q) = (2|q) = (-1)^{(q^2-1)/8}$ since $k = h_1 + h_3 + k_1 + k_3 = 7$. Thus $(q|7) = -1$, $(q|5) = (-1)^{(q^2+7)/8}$ and $q \equiv a_1\Omega_1 \pmod 4$. Take $q = 17$. By (4.77), choose s_2 such that $s_2 = 2s_3$, s_3 odd. By (1.7) and (1.9), $17s_2^2 \equiv -480 \pmod{17}$, and thus $s_2 \equiv \pm 1 \pmod 7$; Take $s_2 = 6$. Then $s_1 = 2^{\epsilon_3/2} s_2 = 6$. By $(1.6)_1$, $A_2 = 156$. By (4.63), $A_2 = 4A_3$, and thus $A_3 = 39$.

By (1.8) and (1.10), $12r_1^2 \equiv -156 \pmod{17}$, and thus $r_1 \equiv \pm 2 \pmod{17}$. By (4.71), choose r_1 such that $r_1^2 \equiv -A_3\gamma_2 \pmod{2}$, where $\gamma_2 \equiv -1 \pmod{4}$ by (4.65). Take $\gamma_2 = -1$. Choose r_1 such that $r_1 \equiv \pm 2 \pmod{17}$ and $r_1 \equiv \pm 1 \pmod{2}$. Take $r_1 = 15$. By (1.11), $c = c_1$. By $(1.6)_2$, $c_1 = 2^3\cdot 3\cdot 7$, and thus $2^3 || c_1$ as asserted by theorem 4.3. By (1.1), $\Omega = 2^3\cdot 3$, $\Delta = 2^3\cdot 5$, $a = 7$ and $b = 2^4\cdot 3\cdot 17$. By (1.12), $s = D_1D_2s_1 = 2\cdot 3$. By (1.13), $r = 2^{\epsilon_1}\Omega_2\Omega_3r_1 = 2^3\cdot 3^2\cdot 5$.

$$d = \begin{vmatrix} 7 & 0 & 2\cdot 3 \\ 0 & 2^4\cdot 3\cdot 17 & 2^3\cdot 3^2\cdot 5 \\ 2\cdot 3 & 2^3\cdot 3^2\cdot 5 & 2^3\cdot 3\cdot 7 \end{vmatrix} = 2^9\cdot 3^2\cdot 5 = \Omega^2\Delta.$$

Example 4.6: [For theorem 4.3 and subcase $(ii)_{13}$ of theorem 1] Summary of subcase is given in example 4.1. Let $\epsilon_1 = 3$, $\epsilon_2 = 0$, $\epsilon_3 = 3$, $\epsilon_4 = 1$, $\Omega_1 = 7$, $\Delta_1 = 5$ and $a_1 = 3$. By (1.2), $\delta_1 = 35$, $D = 1$, $a_2 = 3$, $\delta_2 = 35$, $\Omega_2 = 1$, $\Omega_3 = 7$ and $D_1 = D_2 = 1$. $h_1 = 1$ and $k_3 = 2$. Let $n = 3$, that is, we seek c_1 such that $2^3 || c_1$. $n - k_3 = 1$. Choose $b_2 = q$ an odd prime such that $b_2 \equiv 3\delta_1 \pmod{4}$. By (1.4), $(q|3) = (-35|3) = 1$ since $h = h_2 + h_3 = 0$ and $(q|35\cdot 7\cdot 3) = (-1)^{(q-1)/2\cdot(35\cdot 7\cdot 3 + 1)/2}$ $(2^3|q) = (2|q) = (-1)^{(q^2-1)/8}$ since $k = h_1 + h_3 + k_1 + k_3 = 3$. Thus $(q|3) = 1$, $(q|5) = (-1)^{(q^2-1)/8}$ and $q \equiv 3\delta_1 \pmod{4}$.

Choose $q = 13$. By (1.7) and (1.9), $13s_2^2 \equiv -35 \pmod{6}$, and thus $s_2 \equiv \pm 1 \pmod{6}$. By (4.63) and (4.67), choose s_2 such that $2^3 || (b_2D_2s_2^2 + \delta_2)$. Take $s_2 = 5$. $s_1 = 2^{[(\epsilon'-\epsilon_4+1)/2]} s_2 = 2s_2 = 2\cdot 5$. By $(1.6)_1$, $A_1 = 60$. By (4.63), $A_2 = 15$. By (1.8) and (1.10), $28r_1^2 \equiv -60 \pmod{13}$, and thus $r_1 \equiv \pm 3 \pmod{13}$. By (4.65), $\gamma_2 \equiv -1 \pmod{4}$. Take $\gamma_2 = -1$. By $(4.66)_1$, $r_1^2 \equiv 1 \pmod{2}$. Thus choose $r_1 \equiv \pm 3 \pmod{13}$ and $r_1 \equiv \pm 1 \pmod{2}$. Take $r_1 = 3$. By (1.11), $c = c_1$. By $(1.6)_2$, $c_1 = 2^3\cdot 3$, and thus $2^3 || c_1$ as asserted by theorem 4.3. By (1.1), $\Omega = 2^3\cdot 7$, $\Delta = 5$, $a = 2^3\cdot 3$ and $b = 2^4\cdot 7\cdot 13$. By (1.12), $s = D_1D_2s_1 = 2\cdot 5$. By (1.13), $r = 2^{\epsilon_1}\Omega_2\Omega_3r_1 = 2^3\cdot 3\cdot 7$.

$$d = \begin{vmatrix} 2^3\cdot 3 & 0 & 2\cdot 5 \\ 0 & 2^4\cdot 7\cdot 13 & 2^3\cdot 3\cdot 7 \\ 2\cdot 5 & 2^3\cdot 3\cdot 7 & 2^3\cdot 3 \end{vmatrix} = 2^6\cdot 5\cdot 7^2 = \Omega^2\Delta.$$

Example 4.7: [For theorem 4.3 and subcase $(ii)_{13}$ of theorem 1] Summary of subcase $(ii)_{13}$ is given in example 4.1. Let $\epsilon_1 = 7$, $\epsilon_2 = 1$, $\epsilon_3 = 8$, $\epsilon_4 = 0$, $\Omega_1 = 7$, $\Delta_1 = 5$, $a_1 = 3$ and $b_2 = q$ an odd prime. By (1.2), $\delta_1 = 35$, $D = 1$, $a_2 = 3$, $\delta_2 = 35$, $\Omega_2 = 1$, $\Omega_3 = 7$ and $D_1 = D_2 = 1$. $h_1 = h_2 = h_3 = 0$

and $k_3 = 7$. By (1.4), $(q|3) = (-35|3) = 1$ since $h = h_2 + h_3 = 0$ and $(q|35\cdot 7\cdot 3) = (-1)^{(q-1)/2\cdot(35\cdot 7\cdot 3 + 1)/2}(2^7|q) = (2|q) = (-1)^{(q^2-1)/8}$ since $k = h_1 + h_3 + k_1 + k_3 = 7$. Thus $(q|3) = 1$ and $(q|5) = (-1)^{(q^2-1)/8}$. Choose $q = 13$. By (1.7) and (1.9), $13s_2^2 \equiv -35 \pmod 3$, and thus $s_2 \equiv \pm 1 \pmod 3$. Let $n = 6$, that is, we seek c_1 such that $2^6||c_1$. By (4.93), choose s_2 such that $2^6||(b_2D_2s_2^2 + \delta_2)$, that is, $s_2 \equiv \pm 9 \pmod{64}$ and $s_2 \not\equiv \pm 9 \pmod{128}$. Take $s_2 = 55$. Then $s_1 = 2^{[(\epsilon' - \epsilon_4 + 1)/2]}s_2 = 2^4\cdot 5\cdot 11$. By $(1.6)_1$, $A_1 = 13120$. By (4.91), $A_2 = 205$. By (1.8) and (1.10), $896r_1^2 \equiv -13120 \pmod{13}$, and thus $r_1 \equiv \pm 4 \pmod{13}$. By $(4.92)_2$, choose r_1 different from the solution of $14r_1^2 \equiv -205 \pmod 2$. Thus choose $r_1 \equiv 0 \pmod 2$. Take $r_1 = 4$. By (1.11), $c = c_1$. By $(1.6)_2$, $c_1 = 2^6\cdot 3\cdot 11$, and thus $2^6||c_1$ as asserted by theorem 4.3. By (1.1), $\Omega = 2^7\cdot 7$, $\Delta = 2\cdot 5$, $a = 2^8\cdot 3$ and $b = 2^7\cdot 7\cdot 13$. By (1.12), $s = D_1D_2s_1 = 2^4\cdot 5\cdot 11$. By (1.13), $r = 2^{\epsilon_1}\Omega_2\Omega_3r_1 = 2^9\cdot 7$.

$$d = \begin{vmatrix} 2^8\cdot 3 & 0 & 2^4\cdot 5\cdot 11 \\ 0 & 2^7\cdot 7\cdot 13 & 2^9\cdot 7 \\ 2^4\cdot 5\cdot 11 & 2^9\cdot 7 & 2^6\cdot 3\cdot 11 \end{vmatrix} = 2^{15}\cdot 5\cdot 7^2 = \Omega^2\Delta.$$

Theorem 4.4: Let d, Ω, Δ, a and b be defined as in theorem 1 and let Ω_1 be square free. Then there exists a form in which Ω divides the cofactors of the elements of d if $\epsilon_1 = 0$ or $\epsilon_4 = 0$ or one of the following conditions holds:

(4.107) $\epsilon_1 \leq \epsilon_3 + n_3 < 2n_1$,

(4.108) $\epsilon_1 \leq 2n_1 < \epsilon_3 + n_3$,

(4.109) $\epsilon_1 - \epsilon \leq \epsilon_3 + n_3 = 2n_1$,

where n_1 and n_3 are the exponents of the highest powers of 2 dividing s_1 and c respectively and ϵ is given by

(4.110) $a_1c' - D_1^2D_2^2s_1'^2 = 2^{\epsilon}v$, v odd,

where s_1' and c' are odd and are given by (3.1) and (3.3).

Proof: Let ΩA, ΩB, ΩC, ΩR, ΩS and ΩT be the cofactors of a, b, c, r, s and t (= 0) respectively in d, and thus

$$(4.111) \quad \begin{cases} \Omega A = bc - r^2, \ \Omega B = ac - s^2, \\ \Omega C = ab, \ \Omega R = -ar, \ \Omega S = -bs, \ \Omega T = rs. \end{cases}$$

From (1.1) and (1.13), observe that $\Omega | b$ and $\Omega | r$, and thus Ω divides each of the cofactors in (4.111) except possibly $\Omega B = ac - s^2$.

To determine the conditions under which Ω divides $(ac - s^2)$, consider

(4.112) $d = abc - ar^2 - bs^2$.

From (1.1), (1.2), (1.13) and (4.112), obtain

(4.113) $2^{\epsilon_1}\Omega_3\ (ar_1^2 + \Delta) = 2^{\epsilon_4}b_2\ (ac - s^2).$

Since $(\Omega_3, b_2) = 1$ by theorem 1, (4.113) implies that $\Omega_3 | (ac - s^2)$. From (4.113), observe that if $\epsilon_1 = 0$ or $\epsilon_4 = 0$, then $2^{\epsilon_1}\Omega_3$, that is, Ω divides $(ac - s^2)$.

Next consider the case $\epsilon_1 > 0$ and $\epsilon_4 > 0$. By (1.1), (1.12), (3.1) and (3.3), obtain

(4.114) $ac - s^2 = 2^{\epsilon_3+n_3}a_1c' - 2^{2n_1}D_1^2D_2^2s_1'^2.$

Case (i): $\epsilon_3 + n_3 < 2n_1$. Now (4.114) reduces to

(4.115) $ac - s^2 = 2^{\epsilon_3+n_3}[a_1c' - 2^{2n_1-(\epsilon_3+n_3)}D_1^2D_2^2s_1'^2].$

Thus if $\epsilon_1 \le \epsilon_3 + n_3$, then $\Omega = 2^{\epsilon_1}\Omega_3$ divides $(ac - s^2)$.

Case (ii): $\epsilon_3 + n_3 > 2n_1$. In this case, (4.114) becomes

(4.116) $ac - s^2 = 2^{2n_1}(2^{\epsilon_3+n_3-2n_1}a_1c' - D_1^2D_2^2s_1'^2).$

Hence if $\epsilon_1 \le 2n_1$, then $\Omega | (ac - s^2)$.

Case (iii): $\epsilon_3 + n_3 = 2n_1$. Now (4.114) becomes $ac - s^2 = 2^{\epsilon_3+n_3}(a_1c' - D_1^2D_2^2s_1'^2)$, which reduces to

(4.117) $ac - s^2 = 2^{\epsilon_3+n_3+\epsilon}v$, v odd,

where ϵ is given by (4.110), and thus if $\epsilon_1 \le \epsilon_3 + n_3 + \epsilon$, then $\Omega | (ac - s^2)$. This completes the proof of theorem 4.4.

Remark: From the proof of theorem 4.4, it follows that there exists a form in which Ω does not divide the cofactors of the elements of d if $\epsilon_1 > 0$, $\epsilon_4 > 0$ and one of the following conditions holds:

(4.118) $\epsilon_3 + n_3 < 2n_1$, $\epsilon_1 > \epsilon_3 + n_3$,

(4.119) $\epsilon_3 + n_3 > 2n_1$, $\epsilon_1 > 2n_1$,

(4.120) $\epsilon_3 + n_3 = 2n_1$, $\epsilon_1 > \epsilon_3 + n_3 + \epsilon$.

Some examples of forms in which Ω divides the cofactors of elements of d:

Example 4.8: [For subcase $(i)_{51}$ of theorem 1]
Consider example 4.2 in which $\epsilon_1 = 1$, $\epsilon_3 + n_3 = 2$ and $2n_1 = 4$, and thus (4.107) of theorem 4.4 is satisfied. Note that $\Omega = 2\cdot 7$ divides $ac - s^2 = 2^2\cdot 5\cdot 7$, and thus in the form of this example, Ω divides the cofactors of the elements of d as asserted by theorem 4.4.

Example 4.9: [For subcase $(iv)_{14221}$ of theorem 1]
Consider example 4.3 in which $\epsilon_1 = 2$, $\epsilon_3 + n_3 = 5$ and $2n_1 = 4$, and thus (4.108) of theorem 4.4 is satisfied. Note that $\Omega = 2^2\cdot 3$ divides $ac - s^2 = 2^4\cdot 3\cdot 67$, and thus in the form of this example, Ω divides the cofactors of the elements of d as asserted by theorem 4.4.

Example 4.10: [For subcase $(i)_{51}$ of theorem 1]
Consider example 4.2 in which $s_1 \equiv \pm 1 \pmod 3$. Take $s_1 = 1$. By $(1.6)_1$, $A_1 = 23$. By (1.8) and (1.10), $7r_2^2 \equiv -23 \pmod{3^4}$,

and thus $r_2 \equiv \pm 15 \pmod{3^4}$. Take $r_2 = 15$. Then $r_1 = 2^{(\varepsilon_2-\varepsilon_3)/2} r_2 = 2\cdot3\cdot5$. By $(1.6)_2$ and (1.11), $c = 47$. By (1.12), $s = D_1D_2s_1 = 1$. By (1.13), $r = 2^{\varepsilon_1}\Omega_2\Omega_3 r_1$ $= 2^2\cdot3\cdot5\cdot7$. a, b, Ω and Δ are the same as in example 4.2.

$$d = \begin{vmatrix} 3 & 0 & 1 \\ 0 & 2^5\cdot7\cdot17 & 2^2\cdot3\cdot5\cdot7 \\ 1 & 2^2\cdot3\cdot5\cdot7 & 47 \end{vmatrix} = 2^4\cdot5\cdot7^2 = \Omega^2\Delta.$$

In this example, $\varepsilon_1 = 1$, $\varepsilon_3 + n_3 = 0$, $2n_1 = 0$ and $\varepsilon = 2$ since by (4.111), $a_1c' - D_1^2D_2^2s_1'^2 = 2^2\cdot5\cdot7$, and thus (4.109) of theorem 4.4 is satisfied. Note that $\Omega = 2\cdot7$ divides $ac - s^2 = 2^2\cdot5\cdot7$, and thus in the form of this example, Ω divides the cofactors of the elements of d as asserted by theorem 4.4.

Some examples of forms in which Ω does not divide the cofactors of the elements of d:

Example 4.11: [For subcase $(i)_2$ of theorem 1] Consider example 3.5 in which $\varepsilon_1 = 2$, $\varepsilon_4 = 4$, $\varepsilon_3 + n_3 = 1$ and $2n_1 = 2$, and thus (4.118) is satisfied. Note that $\Omega = 2^2\cdot3$ does not divide $ac - s^2 = 2\cdot3\cdot11$, and thus in the form of this example, Ω does not divide the cofactors of the elements of d as stated in the remark.

Example 4.12: [For subcase $(iii)_{111}$ of theorem 1] Consider example 4.5 in which $\epsilon_1 = 3$, $\epsilon_4 = 1$, $\epsilon_3 + n_3 = 3$ and $2n_1 = 2$, and thus (4.119) is satisfied. Note that $\Omega = 2^3 \cdot 3$ does not divide $ac - s^2 = 2^2 \cdot 3 \cdot 5 \cdot 19$, and thus in the form of this example, Ω does not divide the cofactors of the elements of d as stated in the remark.

Example 4.13: [For subcase $(iii)_{111}$ of theorem 1] Summary of subcase $(iii)_{111}$ is given in example 4.5. Let $\epsilon_1 = \epsilon_2 = 4$, $\epsilon_3 = 2$, $\epsilon_4 = 3$, $\Omega_1 = 5$, $\Delta_1 = 7$, $a_1 = 3$ and $b_2 = q$ an odd prime. By (1.2), $\delta_1 = 35$, $D = 1$, $a_2 = 3$, $\delta_2 = 35$, $\Omega_2 = 1$, $\Omega_3 = 5$ and $D_1 = D_2 = 1$. $h_3 = 3$ and $k_3 = 1$. By (1.4), $(q|3) = (-280|3) = -1$ since $h = h_2 + h_3 = 3$ and $(q|35 \cdot 5 \cdot 3) = (-1)^{(q-1)/2 \cdot (35 \cdot 5 \cdot 3 + 1)/2} = (-1)^{(q-1)/2}$ since $k = h_1 + h_3 + k_1 + k_3 = 4$. Thus $(q|3) = -1$ and $(q|7) = (-1)^{(q+1)/2}$. Choose $q = 11$. By (1.7) and (1.9), $11s_2^2 \equiv -280 \pmod{3}$, and thus $s_2 \equiv \pm 1 \pmod{3}$. Take $s_2 = 1$. Then $s_1 = 2^{\epsilon_3/2} s_2 = 2$. By $(1.6)_1$, $A_2 = 97$. By (1.8) and (1.10), $10r_1^2 \equiv -97 \pmod{11}$, and thus $r_1 \equiv \pm 3 \pmod{11}$. Take $r_1 = 3$. By $(1.6)_2$ and (1.11), $c = c_1 = 17$. By (1.1), $\Omega = 2^4 \cdot 5$, $\Delta = 2^4 \cdot 7$, $a = 2^2 \cdot 3$ and $b = 2^7 \cdot 5 \cdot 11$. By (1.12), $s = D_1 D_2 s_1 = 2$. By (1.13), $r = 2^{\epsilon_1} \Omega_2 \Omega_3 r_1 = 2^4 \cdot 3 \cdot 5$.

$$d = \begin{vmatrix} 2^2\cdot 3 & 0 & 2 \\ 0 & 2^7\cdot 5\cdot 11 & 2^4\cdot 3\cdot 5 \\ 2 & 2^4\cdot 3\cdot 5 & 17 \end{vmatrix} = 2^{12}\cdot 5^2\cdot 7 = \Omega^2\Delta.$$

In this example, $\epsilon_1 = 4$, $\epsilon_4 = 3$, $\epsilon_3 + n_3 = 2$, $2n_1 = 2$ and $\epsilon = 1$ since by (4.111), $a_1c' - D_1^2D_2^2s_1'^2 = 2\cdot 5^2$, and thus (4.120) is satisfied. Now $\Omega = 2^4\cdot 5$ does not divide $ac - s^2 = 2^3\cdot 5^2$, and thus in the form of this example, Ω does not divide the cofactors of the elements of d as stated in the remark.

BIBLIOGRAPHY

1. Jones, B.W. "The Regularity of a Genus of Positive Ternary Quadratic Forms," Transactions of the American Mathematical Society, Vol. 33, 1931, pp. 111 - 124.

2. Hadlock, E.H. "On the Construction of a Ternary Quadratic Form Associated with a Given Determinant," paper presented at Southeastern Section of the Mathematical Association of America, Wake Forest College, Winston-Salem, North Carolina, April 9 - 10, 1965.

3. Dickson, L.E. Introduction to the Theory of Numbers. Chicago: The University of Chicago Press, 1929, p. 13.

BIOGRAPHICAL SKETCH

Syed Asadulla was born on June 3, 1933, in Channapatna, Mysore State, India. He was graduated from Government High School, Channapatna, in June, 1950. He received his degree of Bachelor of Science (Honors) from Central College, Bangalore, India, in April, 1955. He began his graduate studies in mathematics at the University of Karachi, Karachi, Pakistan, in August, 1955, and received his degree of Master of Science in May, 1956. While attending the University of Karachi, he joined the faculty of Syed Raza Ali College (now Federal College), Karachi, where he later held the positions of the head of the Department of Mathematics, chairman of the Faculty of Science and officiating principal. He also worked as co-operative lecturer in mathematics at the University of Karachi from 1957 to 1961 while he was serving Syed Raza Ali College.

In August, 1961, he was offered a scholarship by the United States Educational Foundation in Pakistan and from September, 1961, until the present time he has pursued his work toward the degree of Doctor of Philosophy. He held a graduate assistantship and interim instructorship with the Department of Mathematics and he is now an instructor in the Department of Mathematics.

Syed Asadulla is married to the former Bibijan Khasim. He is a member of the Mathematical Association of America.

This dissertation was prepared under the direction of the chairman of the candidate's supervisory committee and has been approved by all members of that committee. It was submitted to the Dean of the College of Arts and Sciences and to the Graduate Council, and was approved as partial fulfillment of the requirements for the degree of Doctor of Philosophy.

August, 1966

E. Ruffin Jones
Dean, College of Arts and Sciences

Dean, Graduate School

Supervisory Committee:

E. H. Hadlock
Chairman

F. C. Barnett (for W.O. Ash.)
W.R. Hutcherson
T. O. Moore